Finite extensions of algebraic number fields ramify at finitely many primes. The primes that ramify in an extension carry crucial information about the extension. For example, the primes that ramify in the cyclotomic extension $\mathbf{Q}(\zeta_n)$ generated by a primitive n-th root ζ_n of unity for an integer $n \not\equiv 2 \bmod 4$ are precisely the prime divisors of n. The inertia groups at primes dividing n generate the Galois group and this fact implies the surjectivity of the canonical injection $\mathrm{Gal}(\mathbf{Q}(\zeta_n)/\mathbf{Q}) \to (\mathbf{Z}/n\mathbf{Z})^\times$, or equivalently the irreducibility of cyclotomic polynomials. Similarly, for a finite morphism $X \to Y$ of algebraic curves, if the extension of the function fields is separable, there are finitely many points that ramify in the covering.

We distinguish two types of ramifications; tame ramification and wild ramification. Tame ramification is easier to understand and allows geometric intuition similar to the ramification of finite coverings of Riemann surfaces. Tame ramification is determined essentially by the ramification index.

Wild ramification means that the ramification index is divisible by the characteristic of the residue field in the classical setting where the residue field extension is separable, and is much more complicated. In the case of cyclotomic extensions, the ramification is wild if and only if n is divisible by p^2. The understanding of wild ramification inevitably involves additive groups of some vector spaces such as the space of differential forms over the residue fields.

To understand wild ramification, the key tool we use is the filtration by ramification groups. In the case of cyclotomic fields, if we identify the Galois group with $(\mathbf{Z}/n\mathbf{Z})^\times$ by the canonical isomorphism, the congruence modulo powers of prime divisors p of n defines a filtration of the inertia subgroup at each ramified prime p. The fact that this filtration actually gives the ramification groups is the first case of the Hasse–Arf theorem that is at the core of the classical ramification theory.

A main application of the filtration is to the conductor of Galois representations. The integrality of the conductor is proved as a consequence of the Hasse–Arf theorem. We briefly introduce two examples of application of the theory of the conductor, one in number theory and one in algebraic geometry.

In the Langlands correspondence between Galois representations and automorphic representations, the conductor of a Galois representation equals the level of the corresponding automorphic representation. For example, the proof of Fermat's last theorem is completed by proving the modularity of elliptic curves over $\mathbf{Q}$: For an elliptic curve E over $\mathbf{Q}$, there exists a modular form f such that the L-function $L(E, s)$ defined by the Galois representation on the Tate module $T_\ell E$ equals $L(f, s)$. In this correspondence, the conductor of E defined by the ramification of $T_\ell E$ equals the level of f.

In a geometric setting, the conductor appears as the local term in the Grothendieck–Ogg–Shafarevich formula computing the Euler–Poincaré characteristic $\chi_c(U, \mathcal{F})$ of a locally constant étale sheaf $\mathcal{F}$ on a smooth algebraic curve U over an algebraically closed field of characteristic $p > 0$. The local terms are the contributions of points at infinity $X - U$ of the smooth compactification X of U where the sheaf $\mathcal{F}$ ramifies.

In arithmetic geometry, beyond extensions of algebraic number fields or coverings of algebraic curves, we are interested in coverings of schemes of finite type over $\mathbf{Z}$ or those of varieties of higher dimension. Then, contrary to the local fields in the classical setting, the residue fields of local fields are no longer perfect and the residue field extension may be inseparable. This implies that the theory of wild ramification is required to cover extensions such that the extension of residue fields are not separable.

As a geometric application in this general setting, we will give a proof of the Deligne–Kato formula [39] computing the dimension of the space of nearby cycles on a curve over a local field. A special case of the formula plays a crucial role in the proof of the existence of the characteristic cycle of a constructible sheaf on a smooth scheme over a perfect field [61]. As another example of application, the characteristic cycle is known to be computed in codimension 1 by using ramification groups of local fields with imperfect residue fields, loc. cit.

Thus, the main subject of this book is the filtrations by ramification groups of the Galois group of an extension of local fields with no restriction on the residue fields. There are two kinds of ramification groups, the lower numbering ones and the upper numbering ones. They have properties that show sharp contrast:

(1) The lower numbering ramification groups are defined in a fairly elementary way.

Let L be a finite Galois extension of a local field K and G be the Galois group. Then, the inertia subgroup $I \subset G$ is defined as the kernel of the action of G on the residue field $E = \mathcal{O}_L/\mathfrak{m}_L$. As a generalization, a decreasing filtration $G'_i \subset G$ is defined as the kernel of the action of G on $\mathcal{O}_L/\mathfrak{m}_L^i$ indexed by integers $i \geqq 1$. The lower ramification group $G_i \subset G$ is defined as its slight modification obtained by replacing the quotients of the additive group by those $L^\times/(1+\mathfrak{m}_L^i)$ of the multiplicative group. From this definition, we can easily deduce the following facts:

(2) The graded quotients $\mathrm{Gr}_i G = G_i/G_{i+1}$ are $\mathbf{F}_p$-vector spaces for $i \geqq 1$ and $G_i = 1$ for sufficiently large i.

(3) For the subextension $M \subset L$ corresponding to a subgroup $H \subset G$, we have $H_i = H \cap G_i$.

However, in the case where M is a Galois extension of K and hence $H \subset G$ is a normal subgroup:

(4) There is no general way to express the ramification groups $\overline{G}_i \subset \overline{G}$ of the quotient $\overline{G} = G/H = \mathrm{Gal}(M/K)$ out of $G_i \subset G$,

except in the classical case where the ring of integers of the extension is generated by a single element. The properties (3) and (4) indicate that:

(5) The lower numbering filtration is an invariant of L rather than K.

We will see in Section 4.4 that the graded quotients $\mathrm{Gr}_i G$ for $i \geqq 1$ are related to vector spaces over the residue field $E = \mathcal{O}_L/\mathfrak{m}_L$ not over $F = \mathcal{O}_K/\mathfrak{m}_K$.

On the other hand:

(1′) The definition of the upper numbering filtration requires a heavy geometric machinery.

We present a heuristic observation in Section V.0 using the terminology of rigid geometry leading to the definition of upper numbering groups. The actual definition in this book is given entirely in the language of schemes and no knowledge of rigid geometry is required. Still, it requires dilatations, stability of integral models, the going down theorem in commutative algebra etc. The upper ramification subgroups $G^r \subset G$ are indexed by positive rational numbers $r > 0$ and the symbols $r+$ for rational numbers $r \geqq 0$. It is a non-trivial fact that G^1 equals the inertia subgroup I and G^{1+} equals its unique p-Sylow subgroup P called the wild inertia subgroup.

(1″) In the classical case where the ring of integers of the extension is generated by a single element, the upper numbering filtration and the lower numbering filtration are the same up to renumbering controlled by the Herbrand function.

In general, there is no such relation. We will give an elementary counterexample in Section 2.1 as compositions of Artin–Schreier extensions.

The following properties of upper ramification groups are highly non-trivial:

(2′) There exist finitely many rational numbers $1 = r_0 < r_1 < \cdots < r_n$ such that G^r are constant on the intervals $[r_i+, r_{i+1}]$ for $i = 0, \ldots, n-1$ and $G^r = 1$ on $[r_n+, \infty)$.

(2″) The graded quotients $\mathrm{Gr}^r G = G^r/G^{r+}$ are $\mathbf{F}_p$-vector spaces for $r > 1$.

The proof of (2′) requires the reduced fiber theorem and the stable reduction theorem of curves. The proof of (2″) is by the reduction to the classical case where the residue field is perfect and relies on (2) and (1″) above. The reduction requires a study of the first homology group $\mathrm{H}_1(L_{E/\mathcal{O}_K})$ of the cotangent complex which plays the role of the cotangent space at the closed point of the spectrum of the discrete valuation ring. The most difficult case is the case where p is a uniformizer and $dp = 0$ in the usual sense. The introduction of the vector space $\mathrm{H}_1(L_{E/\mathcal{O}_K})$ allows us to avoid this difficulty.

The statements (3) and (4) are switched as follows.

(3′) For the subextension $M \subset L$ corresponding to a subgroup $H \subset G$, there is no general way to express the ramification groups $H^r \subset H$ out of $G^r \subset G$.

In the case where M is a Galois extension of K and hence $H \subset G$ is a normal subgroup, the following property is built in the definition of upper numbering subgroups:

(4′) The ramification groups $\overline{G}^r \subset \overline{G}$ of the quotient $\overline{G} = G/H = \mathrm{Gal}(M/K)$ equal the images of $G^r \subset G$.

The exceptional classical case of (4) is a consequence of (4′) and (1″). The property (4′) indicates:

(5′) The upper numbering filtration is an invariant of K.

In Chapter 14, we will construct an injection called the *characteristic form* from the dual group of the graded quotients $\mathrm{Gr}^r G$ for $r > 1$ to a twist of the vector space $\mathrm{H}_1(L_{E/\mathcal{O}_K})$ that behaves like a scalar extension of that over the residue field $F = \mathcal{O}_K/\mathfrak{m}_K$.

For abelian extensions, Kato defined another filtration [41], which we call the cohomological filtration, using the cup product of abelian characters with the multiplicative group valued in the Brauer group. In the classical case where the residue field is finite, this cohomological filtration is given as the images of $1 + \mathfrak{m}_K^n \subset K^\times$ by the reciprocity morphism $K^\times \to G$ of local class field theory. A feature of the cohomological filtration is the property that the filtration is indexed by integers. Consequently, a comparison of the lower numbering filtration with cohomological filtration implies the integrality of conductor.

For a cyclic extension, under the assumption that the ring of integers is generated by a single element, we prove in Section 4.4 a relation of the cohomological filtration and the lower numbering filtration called the Hasse–Arf theorem. This is proved by induction on the degree of the extension. In the first case where the degree equals the characteristic of the residue field, this is proved by explicit computation for Artin–Schreier extensions in the equal characteristic case and for Kummer extensions in the mixed characteristic case. The induction step is proved by introducing a stronger version due to Kato formulated in terms of a certain twisted differential form called the *refined Swan conductor* defined in [41].

The cohomological filtration shares the property (5′) above with the upper numbering filtration. The refined Swan conductor is a twisted differential form of the residue field $F = \mathcal{O}_K/\mathfrak{m}_K$ with logarithmic pole. We prove in the last chapter of the book a fact proved in [43] that the cohomological filtration and the refined Swan conductor are in fact equal

to logarithmic variants of the upper numbering filtration and of the characteristic form.

In the equal positive characteristic case, by Artin–Schreier–Witt theory describing cyclic extensions of degrees powers of p, the cohomological filtration and the logarithmic variant of the upper numbering filtration admit a concrete description in terms of a filtration on Witt vectors defined by Brylinski [12]. In the mixed characteristic case, we present Kato's theory of the cohomological filtration without giving the details of the proof that relies heavily on computations of p-adic cohomology.

The book consists of fifteen chapters. They are grouped into six parts of the book. Each chapter usually starts with sections preparing some generalities on more basic subjects. In later sections, we apply them to the study of ramification.

In the first two parts, we study the lower numbering filtration and the cohomological filtration. We introduce the two filtrations in Part I and we describe them explicitly for cyclic extensions of degree p in Part II. We prove the Hasse–Arf theorem linking the two filtrations for cyclic extensions under the assumption that the ring of integers is generated by a single element.

In the next two parts, we study applications to Galois representations and to geometric invariants. In Part III, we introduce the conductor of Galois representations using the lower numbering filtration and the Herbrand function and deduce the integrality of the conductor from the Hasse–Arf theorem. In Part IV, we study geometric applications and prove the Grothendieck–Ogg–Shafarevich formula and the Deligne–Kato formula.

In the last two parts, we study the upper numbering filtration. In Part V, after a short introduction on heuristic observation on the construction of the upper numbering filtration using rigid geometry, we construct the filtration in the language of schemes and study its basic properties together with a logarithmic variant. In Part VI, we study the graded quotients using the group structure in the geometric construction and introduce characteristic forms that defines an injection from the dual group of the graded quotients to twisted cotangent spaces.

The last two parts studying upper numbering filtration are almost independent of the first four parts. The geometric results in Chapters 7 and 9 are not used in the rest of the book.

At the end of each chapter, historical notes are included. They are rather personal recollections and the author apologizes for not mentioning many important works. The most part of Chapters 2, 4, 5, 6, 9 and 15 are due to Kazuya Kato and the most part of Chapters 10–13 are done in collaboration with Ahmed Abbes.

Let us now describe the contents of each chapter in more detail. In many books including [65], finite extensions of complete discrete valuation fields are studied. In this book, we replace complete discrete valuation fields by a generalization, henselian discrete valuation fields defined algebraically. Similarly as complete discrete valuation fields, finite extensions of henselian discrete valuation fields are again henselian discrete valuation fields. In Chapter 1, we prepare some generalities on henselian local rings, characterized by Hensel's lemma.

We introduce lower ramification groups in Chapter 1. We prove two formulas under the assumption that the ring of integers is generated by a single element. The first is the relation with the ramification groups of a quotient group and the second is the relation with the different, called the conductor-discriminant formula. The latter is derived from the computation of the trace mapping of the quotient ring of the polynomial ring by a

monic polynomial.

In the classical case where the residue field is finite, the reciprocity morphism of local class field theory is defined by the cup-product with values in the Brauer group, which is canonically identified with $\mathbf{Q}/\mathbf{Z}$ in this case. Chapter 2 begins with an introduction to Brauer groups as Galois cohomology and a brief summary of local class field theory except the theorem of existence. A classical theorem of Hasse gives a relation between the image of the filtration $1 + \mathfrak{m}_L^n$ by the reciprocity morphism and the ramification subgroups.

In Chapter 2, we give a definition of the cohomological filtration by Kato generalizing this classical construction using Galois cohomology. A key construction due to Kato is that of the refined Swan conductor giving an injection from the graded quotients to twisted spaces of differential forms with log poles. We prepare the basic setup in Chapter 2 but postpone the proof of the existence of refined Swan conductor to the last Chapter 15.

We compute explicitly the lower numbering filtration, the cohomological filtration and the refined Swan conductor for cyclic extensions of degree p using Artin–Schreier theory in the equal characteristic case and Kummer theory in the mixed characteristic case in Chapter 3. This computation makes the first step of induction in the proof of the Hasse–Arf theorem in Chapter 4 and is also used in the proof of Epp's theorem in Chapter 8.

To prove the Hasse–Arf theorem, we formulate a stronger form involving the refined Swan conductor. To make the induction work, the first three sections in Chapter 4 are devoted to establishing various compatibilities on the trace of differential forms. We prove an inequality for Swan conductor in general and prove the Hasse–Arf theorem as the equality under the assumption that the ring of integers is generated by a single element.

In Chapter 5, under the classical assumption that the residue field extension is separable, we introduce the conductor of Galois representations and study fundamental properties. We define the conductor by using the break decomposition and the Herbrand function. We prove the integrality of the conductor. In the rank one case, this is a consequence of the Hasse–Arf theorem. The general case is deduced from the rank 1 case by the induction formula. The induction formula is proved by another description of the conductor in terms of the Swan character. This is used as the definition in many books including [66].

In Chapter 6, we introduce a variant of the conductor defined by Kato under the non-classical assumption that the ramification index is 1 and that the residue field extension is generated by a single element. In this setting, the refined Swan conductor is defined as a certain twisted differential form of the residue field. This variant shares the same properties as the conductor studied in Chapter 5. The refined Swan conductor will be used in Chapter 9 to state and prove the Deligne–Kato formula. The refined Swan conductor turns out to be a special case of the characteristic form constructed in general in Chapter 14.

In Chapter 7, we prove the Grothendieck–Ogg–Shafarevich formula computing the Euler–Poincaré characteristic of an étale sheaf on a curve over an algebraically closed field. The conductor defined in Chapter 5 appears as the local term in the formula. The Grothendieck–Ogg–Shafarevich formula is deduced from the Lefschetz trace formula for an endomorphism of a curve. We prove the Lefschetz trace formula in Section 7.1 admitting some basic properties of étale cohomology.

Using the study of cyclic extensions in Chapter 3, we give a proof in Chapter 8 of Epp's theorem: For a transcendental extension of discrete valuation fields, there exists a finite

extension of the base field such that the composition field has ramification index 1 under a certain mild assumption. In a geometric situation, Epp's theorem implies the reduced fiber theorem. This theorem implies a stability of the integral model that is a crucial ingredient in the definition in Chapter 11 of the upper numbering ramification groups. The reduced fiber theorem also plays an important role in the statement of the Deligne–Kato formula.

In Chapter 9, after recalling the definition and some basic properties of nearby cycles functor, we state and give a new local proof of the Deligne–Kato formula computing the dimension of the space of nearby cycles of an étale sheaf on a curve over a local field. The statement uses the refinement of conductor introduced in Chapter 6. Similarly to the proof of the Grothendieck–Ogg–Shafarevich formula, the Deligne–Kato formula is derived from a trace formula and the dimension formula in the constant coefficient case. These two formulas are deduced directly from the Picard–Lefschetz formula in the case where the curve over the discrete valuation ring is nodal, i. e. with at most nodes as singularities. The general case is reduced to this case by a local version due to Temkin of the stable reduction theorem of curves. The new point in the proof in this book is that we take a blow-up avoiding taking compactification.

From Chapter 10 on, we study upper ramification groups. We define the upper ramification groups in Chapters 10 and 11. To define subgroups G^r for $r > 0$ and G^{r+} for $r \geqq 0$ of the Galois group $G = \mathrm{Gal}(L/K)$, it suffices to define quotient functors F^r and F^{r+} of the fiber functor F sending subextensions $M \subset L$ to the finite set $F(M) = \mathrm{Mor}_K(M, L)$ and to verify that F^r and F^{r+} satisfy certain properties. For $r > 0$, to define the set $F^r(M)$, first we take an immersion $T = \mathrm{Spec}\, \mathcal{O}_M \to Q$ into a smooth scheme over $S = \mathrm{Spec}\, \mathcal{O}_K$ and construct a dilatation $Q_{\overline{S}}^{[r]}$ with respect to the multiplicity r, of the base change $Q_{\overline{S}} = Q \times_S \overline{S}$ to $\overline{S} = \mathrm{Spec}\, \mathcal{O}_{K_s}$ for the ring of integers in a separable closure. Then, $F^r(M)$ is defined as the set $\pi_0(Q_{\overline{F}}^{(r)})$ of connected components of the geometric closed fiber of the normalization $Q_{\overline{S}}^{(r)}$ of $Q_{\overline{S}}^{[r]}$. For $r \geqq 0$, the immersion $T \to Q$ induces a morphism $\overline{T}_{\overline{S}} \to Q_{\overline{S}}^{(r)}$ of normalizations and the set $F^{r+}(M)$ is defined as the image of the restriction of the morphism on the closed fibers.

In Chapter 10, we study this geometric construction. The fact that the functor $F^r(M)$ is defined independently of the choice of the immersion $T \to Q$ is a consequence of a homotopy property of the construction of dilatations. The existence of the stable integral model is a consequence of the reduced fiber theorem proved in Chapter 8. The property of the functors F^r and F^{r+} used to define the subgroups G^r and G^{r+} is a consequence of the going down theorem in commutative algebra.

We compute the geometric construction explicitly in the case where the ring of integers is generated by a single element and observe the appearance of the Herbrand function. This implies property $(1'')$. We also prove the equalities $G^1 = I$ and $G^{1+} = P$. After recalling the general form of the reduced fiber theorem, we prove property $(2')$ above to close Chapter 11.

In Chapter 12, we study a logarithmic variant of the construction in Chapter 11. First, we introduce some generalities on log smooth schemes over $S = \mathrm{Spec}\, \mathcal{O}_K$ and on log smooth extensions of K without using the general theory of log geometry. Then by replacing an immersion $T \to Q$ into a smooth scheme by an exact immersion into a log smooth scheme, we define a logarithmic variant of the upper ramification groups. In the second half of Chapter 12, we focus on Artin–Schreier–Witt extensions in characteristic $p > 0$. We give a geometric proof of the fact that Brylinski's filtration induces the logarithmic upper

numbering filtration.

In Chapters 13 and 14, we study the graded quotients $\mathrm{Gr}^r G = G^r/G^{r+}$ for $r > 1$. We prove property $(2'')$ above in Chapter 13 and we study a construction of injection of the dual group to a twisted 'cotangent' space in Chapter 14. Chapter 13 begins with the study of $\mathrm{H}_1(L_{E/S})$ that plays the role of the cotangent space at the closed point of $S = \operatorname{Spec} \mathcal{O}_K$.

The tool we use to study the graded quotients $\mathrm{Gr}^r G$ is the reduced geometric closed fiber $Q^{(r)}_{\overline{F}} \to Q^{[r]}_{\overline{F},\mathrm{red}}$ of the morphism to the dilatation from the normalization. The target $Q^{[r]}_{\overline{F},\mathrm{red}}$ is a twist of the fiber $N_{T/Q} \otimes_{\mathcal{O}_L} \overline{F}$ of the conormal sheaf of an immersion $T = \operatorname{Spec} \mathcal{O}_L \to Q$ into a smooth scheme over $S = \operatorname{Spec} \mathcal{O}_K$. If the immersion is minimal in the sense that $\dim Q$ is minimal, the canonical injection $\mathrm{Tor}_1^{\mathcal{O}_L}(\Omega^1_{\mathcal{O}_L/\mathcal{O}_K}, \overline{F}) \to N_{T/Q} \otimes_{\mathcal{O}_L} \overline{F}$ is an isomorphism and a connected component $Q^{[r]}_{\overline{F},\mathrm{red}}$ is canonically identified with a vector space denoted $\Theta^{(r)\circ}_{L/K,\overline{F}}$. This space is linked to $\mathrm{H}_1(L_{\overline{F}/S})$ by the injection $\mathrm{Tor}_1^{\mathcal{O}_L}(\Omega^1_{\mathcal{O}_L/\mathcal{O}_K}, \overline{F}) \to \mathrm{H}_1(L_{\overline{F}/S})$ defined by the functoriality of cotangent complexes.

By the compatibility $(4')$ with the quotient, the study of the graded quotients $\mathrm{Gr}^r G$ is reduced to the study of the last piece G^r of the filtration satisfying $G^{r+} = 1$. Under this condition, the crucial property is that the finite morphism $Q^{(r)}_{\overline{F}} \to Q^{[r]}_{\overline{F},\mathrm{red}}$ is étale. This for a minimal immersion $T \to Q$ defines a G^r-torsor $\Phi^{(r)\circ}_{L/K,\overline{F}} \to \Theta^{(r)\circ}_{L/K,\overline{F}}$. By using the functoriality of this G^r-torsor, we first prove that G^r is abelian.

In the classical case where the residue field is perfect, the relation $(1'')$ of the upper and lower ramification groups together with (2) implies property $(2'')$. We prove the general case of $(2'')$ by the reduction to this case. By the functoriality of the construction in the previous paragraph, this is proved by constructing an extension of henselian discrete valuation field with perfect residue field such that the morphism on the 'cotangent' space $\mathrm{H}_1(L_{E/S})$ is an injection.

By the description of the extension group of a vector space by a finite $\mathbf{F}_p$-vector space prepared in the first sections in Chapter 13, the definition of the characteristic form is reduced to showing that the G^r-torsor $\Phi^{(r)\circ}_{L/K,\overline{F}} \to \Theta^{(r)\circ}_{L/K,\overline{F}}$ is in fact an isogeny of group schemes. In this book, we prove this result only in the case where K is of characteristic $p > 0$ and r is an integer and refer to [62] in the general case. The case above is reduced to the case where K is a local field at the generic point of a smooth divisor in a smooth scheme over a perfect field. In this geometric case, the group structure arises from the groupoid structure of self-products at the boundary of the dilatation.

In Chapter 15, we study a logarithmic variant. We also study the cohomological filtration for abelian extensions and its relation with the logarithmic variant. In the equal characteristic $p > 0$ case, the cohomological filtration is also induced by Brylinski's filtration on Witt vectors. This and the result in Chapter 12 imply the equality of the logarithmic upper numbering filtration and the cohomological filtration. We give a proof with Kato of the equality also in the mixed characteristic case. By the functoriality of the logarithmic characteristic form and the refined Swan conductor, the proof is reduced to the case where the ramification index is one and the ring of integers is generated by a single element. In this case, the equality follows from the Hasse–Arf theorem and property $(1'')$. To assure the existence of a suitable extension in the reduction, we apply Epp's theorem proved in Chapter 8. In the final section, we sketch an outline of the proof by Kato of the existence of refined Swan conductor.

Throughout the book, we assume basic knowledge on commutative algebra. We recall basic properties of étale morphisms in Section 1.1. Although we also use the language of schemes, in the most part, it is limited to affine schemes. Exceptions are Chapters 7 and 9 where we use proper curves and blow-ups respectively. In Chapter 7, we also use étale cohomology admitting its basic properties. We briefly recall the definition and basic properties of nearby cycles in Section 9.2.

In Chapter 2, we freely use Galois cohomology as in [65, Chapitre X] including cup-product and the inflation-restriction sequence. We also use some fundamental facts on differential forms in characteristic $p > 0$. In Part III, we assume basic knowledge on representations of finite groups as in [66, Partie III]. We briefly recall the theory of Brauer trace of modular representations in Section 5.1.

In Chapter 11, it is not necessary but will be useful to be familiar with the terminology of Galois categories and fiber functors. In Chapters 12 and 15, we introduce the terminology of log geometry but the knowledge of its generality is not required. In the second half of Chapter 12, we also use Artin–Schreier–Witt theory and Witt vectors. In Chapter 13, we use some elementary homological algebra including Tor and cotangent complexes. We only use basic properties and it is not necessary to go back to the construction. We also use interpretation of H^1 in terms of torsors in Chapter 13 and Artin–Schreier coverings in characteristic $p > 0$. In Chapter 14, we use terminology of group schemes and groupoids.

The author thanks Hiroki Kato for helping preparing the manuscript of Chapter 9.

Contents

Part I
Ramification of henselian discrete valuation fields

We study elementary properties on ramification of finite extensions of henselian discrete valuation fields. Complete discrete valuation fields are henselian discrete valuation fields and similarly to the former, the rings of integers of finite extensions of the latter are again discrete valuation rings.

We define the lower ramification groups of the Galois groups of finite Galois extensions of henselian discrete valuation fields. We prove an equality giving a relation with the filtration on quotient groups under the assumption that the ring of integers is generated by a single element. We also define the different of finite separable extensions and show its relation with lower ramification groups under the same assumption. These relations will imply the compatibility with quotient groups of Swan conductor in Part III.

We introduce a filtration on the character group of the abelian quotient of the absolute Galois group. This is defined as the dual of the filtration on the multiplicative group, using the pairing with values in the Brauer group defined by the cup product of Galois cohomology. In the classical case where the residue field is finite, the pairing induces the reciprocity mapping of local class field theory.

Similarly as the p-torsion part of the unramified part of the character group receives a surjection from the additive group of the residue field by the Artin–Schreier theory, the p-torsion part of the unramified part of the Brauer group receives a surjection from the group of differential forms of the residue field with logarithmic poles. Using this fact, we study the graded pieces of the cohomological filtration and introduce the refined Swan conductor.

1 Finite extensions

The ramification theory for complete discrete valuation fields works equally for henselian discrete valuation fields. A main reason to consider henselian discrete valuation rings is the equivalence (1)$\Leftrightarrow$(3) in Proposition 1.4.4 on the integral closures in finite extensions.

Before introducing henselian local rings in Section 1.3, we prepare fundamental properties of étale morphisms of rings in Section 1.1. We study basic properties of finite extensions of henselian discrete valuation fields in Section 1.4.

We define the lower ramification groups in Section 1.6. The inertia group G_0 and the wild inertia group G_1 correspond to the maximum unramified extension and the maximum tamely ramified extension introduced in Section 1.5. The lower ramification groups provide a tool to study the wild inertia group.

We define the different in Section 1.7 and give a criterion in terms of the different for an extension to be unramified or tamely ramified. We will compute the different explicitly using the derivative of the minimal polynomial of a generator of the ring of integers, using the computation of the trace mapping prepared in Section 1.2. We also study in Section 1.8 some basic properties on the norm mapping and the filtration on the multiplicative groups.

1.1 Étale algebras

Definition 1.1.1. *Let $A \to B$ be a morphism of rings.*

1. *The B-module $\Omega^1_{B/A}$ of differential forms is defined as $J \otimes_{B \otimes_A B} B$ where J is the kernel of the surjection $B \otimes_A B \to B$ sending $x \otimes y$ to xy.*

2. *We say that B is of finite presentation over A, if there exists an isomorphism $A[X_1, \ldots, X_n]/(f_1, \ldots, f_m) \to B$ of rings over A.*

Proposition 1.1.2. *Let $A \to B$ be a morphism of rings.*

1. *The B-module $\Omega^1_{B/A}$ represents the functor $\mathrm{Der}_A(B, -)\colon (B\text{-modules}) \to (\mathrm{Sets})$ sending a B-module M to*

$$\mathrm{Der}_A(B, M) = \{d \in \mathrm{Hom}_A(B, M) \mid d(xy) = xdy + ydx \text{ for any } x, y \in B\}.$$

2. *Let $B = A[X_1, \ldots, X_n]/(f_1, \ldots, f_m)$ and regard the Jacobian matrix $D = \left(\dfrac{\partial f_i}{\partial X_j}\right) \in \mathrm{M}(m, n, B)$ as a B-linear morphism $B^n \to B^m$. Then, $dX_1, \ldots, dX_n \in \Omega^1_{B/A}$ defines a B-linear isomorphism $\mathrm{Coker}(D^\vee\colon B^m \to B^n) \to \Omega^1_{B/A}$.*

Proof. 1. For a B-module M, regard $B \oplus M$ as a ring over B by $xy = 0$ for $x, y \in M$. Then, the mapping $\mathrm{Mor}_A(B, B \oplus M) \to \mathrm{Hom}_A(B, M)$ sending f to $\mathrm{pr}_2 \circ f$ induces a bijection $P = \{f \in \mathrm{Mor}_A(B, B \oplus M) \mid \mathrm{pr}_1 \circ f = 1_B\} \to \mathrm{Der}_A(B, M)$. Let $i_1, i_2\colon B \to B \otimes_A B$ be the morphisms defined by $i_1(b) = b \otimes 1$ and $i_2(b) = 1 \otimes b$ and regard $B \otimes_A B$ as a ring over B by i_2. Then, by the universality of tensor product, the set P is identified with $Q = \{g \in \mathrm{Mor}_B(B \otimes_A B, B \oplus M) \mid \mathrm{pr}_1 \circ g \circ i_1 = 1_B\}$ by sending g to $g \circ i_1$. Since $(B \otimes_A B)/J^2 = B \oplus (J/J^2)$, the set Q is further identified with $\mathrm{Hom}_B(J/J^2, M)$. Hence the assertion follows.

2. Let $x_i \in B$ be the images of X_i. It suffices to show that, for a B-module M, the mapping $\mathrm{Der}_A(B, M) \to M^n$ sending a derivation d to (dx_i) induces a bijection $\mathrm{Der}_A(B, M) \to \mathrm{Ker}(D\colon M^n \to M^m)$. In the case $m = 0$, $s_1, \ldots, s_n \in M$ defines uniquely a derivation $A[X_1, \ldots, X_n] \to M$ sending g to $\sum_j \dfrac{\partial g}{\partial X_j} s_j$. In the general case, the derivation $d\colon A[X_1, \ldots, X_n] \to M$ defined by $s_1, \ldots, s_n \in M$ factors though the surjection $A[X_1, \ldots, X_n] \to B$ if and only if $df_i = \sum_j \dfrac{\partial f_i}{\partial X_j} s_j$ is 0 for $i = 1, \ldots, m$. This means that $(s_1, \ldots, s_n) \in M^n$ lies in the kernel of D. Hence the assertion follows. □

We give a functorial characterization of rings of finite presentation.

Lemma 1.1.3. *Let $A \to B$ be a morphism of rings. The following conditions are equivalent:*

(1) *B is of finite presentation over A.*

(2) *For any filtered inductive system $(C_\lambda)_{\lambda \in \Lambda}$ of rings over A, the canonical mapping $\varinjlim_{\lambda \in \Lambda} \mathrm{Mor}_A(B, C_\lambda) \to \mathrm{Mor}_A(B, \varinjlim_{\lambda \in \Lambda} C_\lambda)$ is a bijection.*

Proof. (1)⇒(2): We show the surjectivity. Let $g\colon B = A[X_1, \ldots, X_n]/(f_1, \ldots, f_m) \to C = \varinjlim_{\lambda \in \Lambda} C_\lambda$ be a morphism over A. Since $(C_\lambda)_{\lambda \in \Lambda}$ is filtered, there exist $\lambda \in \Lambda$ and $x_1, \ldots, x_n \in C_\lambda$ such that their images are $g(X_1), \ldots, g(X_n) \in C$. Define $\widetilde{g}_\lambda\colon A[X_1, \ldots, X_n] \to C_\lambda$ by $x_1, \ldots, x_n \in C_\lambda$. Further, there exists $\mu \geqq \lambda$ such that the composition $\widetilde{g}_\mu\colon A[X_1, \ldots, X_n] \to C_\mu$ maps $f_1, \ldots, f_m$ to 0 and hence induces $g_\mu\colon B \to C_\mu$. Then, the image of (g_μ) is g.

We show the injectivity. Let (g_λ) and (h_λ) be two elements of $\varinjlim_{\lambda\in\Lambda} \mathrm{Mor}_A(B, C_\lambda)$ with the same image $g\colon B \to C$. Then, since $g(X_i) = h(X_i)$ for $i = 1, \ldots, n$ and $(C_\lambda)_{\lambda\in\Lambda}$ is filtered, there exists $\mu \in \Lambda$ such that $g_\mu(X_i) = h_\mu(X_i)$ for $i = 1, \ldots, n$. Hence we have $(g_\lambda) = (h_\lambda)$.

(2)⇒(1): Let $(B_\lambda)_{\lambda\in\Lambda}$ be the inductive system of subrings of B of finite type over A. Then, since the identity of B is factorized as $B \to B_\lambda \to B$ for some $\lambda \in \Lambda$, it follows that $B = B_\lambda$ is of finite type over A. Let $C = A[X_1, \ldots, X_n] \to B$ be a surjection and I be the kernel. Let $(I_\lambda)_{\lambda\in\Lambda}$ be the inductive system of subideals of I of finite type. Then, we have an isomorphism $\varinjlim_{\lambda\in\Lambda} C/I_\lambda \to B = C/I$. The identity of B is factorized as $B \to C/I_\lambda \to B = C/I$ for some $\lambda \in \Lambda$. Further, there exists $\mu \geqq \lambda$ such that the composition $C \to B \to C/I_\mu$ is the canonical surjection. Then, it follows that $I = I_\mu$ is of finite type. □

Definition 1.1.4. *Let $A \to B$ be a morphism of rings.*

1. *We say that B is étale over A if B is of finite presentation over A, if B is flat over A and if $\Omega^1_{B/A} = 0$.*

2. *Let $\mathfrak{q}$ be a prime ideal of B. We say that B is étale over A at $\mathfrak{q}$ if there exists an element $b \in B - \mathfrak{q}$ such that $B[1/b]$ is étale over A.*

A ring B of finite presentation over A is étale over A if and only if it is étale over A at every prime ideal. If B is étale over A, for another ring A' over A, the tensor product $B' = B \otimes_A A'$ is étale over A'. Conversely, if A' is faithfully flat over A and if B' is étale over A', then B is étale over A.

We give examples of rings étale over A.

Lemma 1.1.5. *Let A be a ring, $P \in A[X]$ be a polynomial and P' be the derivative. Then, the ring $B = A[X]/(P)[P'^{-1}]$ is étale over A.*

Proof. Since B is isomorphic to $A[X, Y]/(P, P'Y - 1)$ over A, it is of finite presentation over A. Further B is flat over A by [25, Chapitre 0_{III} (10.2.4) b)⇒ a)]. Since the B-module $\Omega^1_{B/A}$ is generated by dX and its annihilator is $(P') = B$ by Lemma 1.1.2.2, the assertion follows. □

To give a local description of étale morphisms, we show properties of idempotents.

Lemma 1.1.6. *Let A be a ring.*

1. *For an ideal $I \subset A$, the following conditions are equivalent:*

(1) *I is finitely generated and $I = I^2$.*

(2) *There exists an idempotent $e \in A$ such that $I = (1 - e)$.*

2. *Let B be a ring of finite type over A and $B \to A$ be a morphism over A such that $\Omega^1_{B/A} \otimes_B A = 0$. Then there exists an idempotent e of B such that $\mathrm{Ker}(B \to A) = (1-e)B$.*

Proof. 1. (1)⇒(2): Let $x_1, \ldots, x_n$ be a system of generators of I. Since $I = I^2$, there exists $a_{ij} \in I$ such that $x_i = \sum_{j=1}^n a_{ij}x_j$ for $i = 1, \ldots, n$. Namely, the matrix $\boldsymbol{A} \in M(n, A)$ with entries $a_{ij} \in I$ and the column vector $\boldsymbol{x} \in A^n$ with entries $x_i \in I$ satisfy $\boldsymbol{x} = \boldsymbol{A}\boldsymbol{x}$. Hence, we have $e = \det(1_n - \boldsymbol{A}) \equiv 1 \bmod I$ and $e \cdot \boldsymbol{x} = 0$. Thus, the ideal $I' = (e)$ satisfies $A = I' + I$ and $II' = 0$. Hence we obtain $A = A/I \times A/I'$ by the Chinese remainder theorem and $e \in A$ corresponds to $(1, 0)$.

(2)⇒(1): The ideal I is generated by an idempotent $1 - e$.

2. Let I be the kernel of the surjection $B \to A$ and J be the kernel of the surjection $B \otimes_A B \to B$. Since B is of finite type over A, the ideal $I \subset B$ is finitely generated. Since $I = JB$ and $\Omega^1_{B/A} = J/J^2$, we have $I/I^2 = J/J^2 \otimes_B A = 0$. Since $I = I^2$, there exists an idempotent $e \in B$ such that $\mathrm{Ker}(B \to A) = (1-e)B$ by 1. □

Étale algebras over a field are products of finite separable extensions.

Proposition 1.1.7. *Let k be a field and B be a ring of finite type over k.*

1. *For a prime ideal $\mathfrak{q} \subset B$, the following conditions are equivalent:*

(1) *B is étale over k at $\mathfrak{q}$.*

(2) *The quotient ring $B/\mathfrak{q}$ is a finite separable extension of k and B is isomorphic to a product ring $B/\mathfrak{q} \times B'$.*

2. *The following conditions are equivalent:*

(1) *B is étale over k.*

(2) *B is isomorphic over k to a product of finitely many finite separable extensions of k.*

Proof. 1. (2)⇒(1): We may assume that B is a finite separable extension of k. Then, we have a separable irreducible polynomial $P \in k[X]$ and an isomorphism $k[X]/(P) \to B$ over k. Hence the assertion follows from Lemma 1.1.5.

(1)⇒(2): First, we assume that k is an algebraically closed field. Let $\mathfrak{n} \supset \mathfrak{q}$ be a maximal ideal. Then by Lemma 1.1.6.2, we have an isomorphism $B \to B/\mathfrak{n} \times B'$. Hence, we have $\mathfrak{n} = \mathfrak{q}$ and the assertion follows in this case.

By the case where k is an algebraically closed field, every point of $\mathrm{Spec}\,(B/\mathfrak{q}) \otimes_k \overline{k}$ is an isolated point. Since $\mathrm{Spec}\,(B/\mathfrak{q}) \otimes_k \overline{k}$ is quasi-compact, the ring $(B/\mathfrak{q}) \otimes_k \overline{k}$ is a product of finitely many copies of k and further $B \otimes_k \overline{k}$ is isomorphic to a product $(B/\mathfrak{q}) \otimes_k \overline{k} \times B_1$. Hence $B/\mathfrak{q}$ is a finite separable extension of k and B is isomorphic to a product ring $B/\mathfrak{q} \times B'$.

2. (1)⇒(2): By 1 (1)⇒(2), every point of $\mathrm{Spec}\, B$ is an isolated point. Since $\mathrm{Spec}\, B$ is quasi-compact, the assertion follows.

(2)⇒(1): Clear from 1 (2)⇒(1). □

We prove the local description below using Zariski's main theorem.

Theorem 1.1.8. (Zariski's main theorem, [54, Chapitre IV, Théorème 1, Corollaire 1]). *Let $f\colon A \to B$ be a morphism of rings such that B is of finite type over A. Let $\mathfrak{q} \subset B$ be a prime ideal and $\mathfrak{p} = f^{-1}(\mathfrak{q}) \subset A$. Assume that $\mathfrak{q}$ is an isolated point of the fiber $\mathrm{Spec}\, B \otimes_A k(\mathfrak{p})$.*

Then, there exist a subring $B' \subset B$ finite over A and an element $b \in B' - (B' \cap \mathfrak{q})$ such that the inclusion $B'[1/b] \to B[1/b]$ is an isomorphism.

Theorem 1.1.9. ([26, Théorème (18.4.6)], [54, Chapitre V, §1, Théorème 1.1]). *Let $f\colon A \to B$ be a morphism of rings such that B is of finite presentation over A. Let $\mathfrak{q} \subset B$ be a prime ideal and $\mathfrak{p} = f^{-1}(\mathfrak{q}) \subset A$. Then, the following conditions are equivalent:*

(1) *B is étale over A at $\mathfrak{q}$.*

(2) *There exist a monic polynomial $P \in A_{\mathfrak{p}}[T]$, a maximal ideal $\mathfrak{n}$ of $C = A_{\mathfrak{p}}[T]/(P)$ not containing P' and an isomorphism $C_{\mathfrak{n}} \to B_{\mathfrak{q}}$ over $A_{\mathfrak{p}}$.*

Proof. (1)⇒(2): By Proposition 1.1.7.1 and Theorem 1.1.8, we may assume that B is finite over A. By replacing A by the localization $A_{\mathfrak{p}}$, we may assume that A is local and that $\mathfrak{p}$ is the maximal ideal.

By Proposition 1.1.7.1, $B/\mathfrak{q}$ is a finite separable extension of $F = A/\mathfrak{p}$ and $B/\mathfrak{p}B$ is a product ring $B/\mathfrak{q} \times B'$. Hence, there exists $x \in B - \mathfrak{q}$ such that $B/\mathfrak{q}$ is generated by x over $A/\mathfrak{p}$ and that the image of x in B' is 0. Since B is finite over A, the element x is integral over A and the subring $A[x] \subset B$ generated by x is also finite. Let $n = \dim_F A[x] \otimes_A F$. Then, $1, x, \ldots, x^{n-1}$ is a basis of $A[x] \otimes_A F$ and the A-module $A[x]$ is generated by $1, x, \ldots, x^{n-1}$ by Nakayama's lemma. Hence, there exists a monic polynomial $P \in A[X]$ of degree n and a surjection $C = A[X]/(P) \to A[x] \subset B$.

Let $\mathfrak{n} \subset C$ be the inverse image of $\mathfrak{q} \subset B$. Since $\mathfrak{q} \in \operatorname{Spec} B$ is a unique point above $\mathfrak{n} \in \operatorname{Spec} C$ and since the morphism $C/\mathfrak{n} \to B/\mathfrak{n}B = B/\mathfrak{q}$ is an isomorphism, the finite morphism $C_\mathfrak{n} \to B \otimes_C C_\mathfrak{n}$ is a surjection by Nakayama's lemma. The quotient ring $B \otimes_C C_\mathfrak{n}$ of $C_\mathfrak{n}$ is a local ring and hence we have $B \otimes_C C_\mathfrak{n} = B_\mathfrak{q}$. Since C and an open neighborhood of $\operatorname{Spec} B$ are flat of finite presentation over A and since $C/\mathfrak{n} = C_\mathfrak{n}/\mathfrak{p}C_\mathfrak{n} \to B/\mathfrak{q} = B_\mathfrak{q}/\mathfrak{p}B_\mathfrak{q}$ is an isomorphism, the local morphism $C_\mathfrak{n} \to B_\mathfrak{q}$ is flat by [26, Théorème (11.3.10)] and is injective. Hence the morphism $C_\mathfrak{n} \to B_\mathfrak{q}$ is an isomorphism. Since $\Omega^1_{C/A} \otimes_C k(\mathfrak{n}) = 0$, we have $P' \notin \mathfrak{n}$.

(2)⇒(1): The isomorphism $C_\mathfrak{n} \to B_\mathfrak{q}$ is extended to an isomorphism $C[1/c] \to B[1/b]$ over A for $b \in B - \mathfrak{q}, c \in C - \mathfrak{n}$ by Lemma 1.1.3. Hence the assertion follows from Lemma 1.1.5. □

We omit the proof of the following functorial characterization of étale morphisms.

Theorem 1.1.10. ([26, Théorème (17.6.1)], [54, Chapitre V, §1, Théorème 2, Corollaire 1]). *Let $f\colon A \to B$ be a morphism of rings such that B is of finite presentation over A. The following conditions are equivalent:*

(1) *B is étale over A.*

(2) *For any ring C over A and any ideal $I \subset C$ such that $I^2 = 0$, the surjection $C \to C/I$ induces a bijection $\operatorname{Mor}_A(B, C) \to \operatorname{Mor}_A(B, C/I)$ of the sets of morphisms of rings over A.*

Lemma 1.1.11. *Let $A \to B$ be a morphism of rings and assume that B is free of finite rank as an A-module. Then, the functor F sending a ring C over A to the set $\operatorname{Idem}(B \otimes_A C)$ of idempotents is representable by a ring E étale over A.*

Proof. Let $b_1, \ldots, b_n$ be a basis of the A-module B. Let $A[x_1, \ldots, x_n]$ be a polynomial ring and let $x = \sum_{i=1}^n x_i \otimes b_i \in A[x_1, \ldots, x_n] \otimes_A B$ be the universal section. Then, the functor F is represented by the quotient E of $A[x_1, \ldots, x_n]$ by the ideal generated by the coefficients of $b_1, \ldots, b_n$ in $x^2 - x \in A[x_1, \ldots, x_n] \otimes_A B$. The ring E is of finite presentation over A.

We show that E is étale over A. In the case $B = A$ and $b_1 = 1$, we have $E = A[X]/(X^2 - X)$. Since E is isomorphic to $A \times A$ by the Chinese remainder theorem, E is étale over A.

We show the general case. Since the case $B = A$ is already proved, for any ring C over A and any ideal $I \subset C$ satisfying $I^2 = 0$, the surjection $C \to C/I$ induces a bijection $\operatorname{Idem} C \to \operatorname{Idem} C/I$ by Theorem 1.1.10 (1)⇒(2). Applying this to the surjection $B \otimes_A C \to B \otimes_A C/I$, we see that $F(C) \to F(C/I)$ is also a bijection. Hence E is étale over A by Theorem 1.1.10 (2)⇒(1). □

Exercise 1.1. Let $p > 2$ be a prime number and ζ_p be a primitive p-th root of 1. Find the prime ideals of $\mathbf{Z}[\zeta_p]$ where $\mathbf{Z}[\zeta_p]$ is not étale over $\mathbf{Z}$.

Solution. Since $\mathbf{Z}[1/p][X]/(X^p-1) = \mathbf{Z}[\zeta_p][1/p] \times \mathbf{Z}[1/p]$ and $(X^p-1)' = pX^{p-1}$ is invertible in $\mathbf{Z}[1/p][X]/(X^p-1)$, we see that $\mathbf{Z}[\zeta_p][1/p]$ is étale over $\mathbf{Z}$ by Lemma 1.1.5. Since $\mathbf{Z}[\zeta_p] \otimes_{\mathbf{Z}} \mathbf{F}_p$ is isomorphic to $\mathbf{F}_p[X]/(X^{p-1})$ and is not étale over $\mathbf{F}_p$ for $p-1>1$, we see that $\mathbf{Z}[\zeta_p]$ is not étale over $\mathbf{Z}$ at the prime ideal $(\zeta_p - 1)$.

1.2 Trace

We compute the trace mapping for the quotient ring of a polynomial ring by a monic polynomial.

Lemma 1.2.1. *Let A be a ring and let $P \in A[X]$ be a monic polynomial of degree n. Let $b \in B = A[X]/(P)$ be the image of $X \in A[X]$ and define $c_0 = 1, c_1, \ldots, c_{n-1} \in B$ by $P = (X-b) \cdot (c_0 X^{n-1} + \cdots + c_{n-1})$.*

1. *The sequence $c_0 = 1, c_1, \ldots, c_{n-1}$ is a basis of a free A-module B.*
2. *The B-module $\mathrm{Hom}_A(B, A)$ is a free module of rank 1. Let $f_0, \ldots, f_{n-1} \in \mathrm{Hom}_A(B, A)$ be the dual basis of the basis $c_0 = 1, c_1, \ldots, c_{n-1}$ as a free A-module. Then $f_{n-1} \in \mathrm{Hom}_A(B, A)$ is a basis as a free B-module and we have $f_i = b^{n-1-i} f_{n-1}$ for $i = 0, \ldots, n-1$.*
3. *Let $g_0, \ldots, g_{n-1} \in \mathrm{Hom}_A(B, A)$ be the dual basis of the basis $b^0 = 1, b, \ldots, b^{n-1}$ as a free A-module. Then, we have $g_i = c_{n-1-i} f_{n-1}$.*

Proof. 1. Let $P = X^n + a_1 X^{n-1} + \cdots + a_n \in A[X]$. Then since $P = P - P(b) = (X^n - b^n) + a_1(X^{n-1} - b^{n-1}) + \cdots + a_{n-1}(X-b)$, we have

$$\begin{pmatrix} 1 \\ c_1 \\ \vdots \\ c_{n-1} \end{pmatrix} = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ a_1 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ a_n & \cdots & a_1 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ b \\ \vdots \\ b^{n-1} \end{pmatrix} \tag{1.1}$$

Since $1, b, \ldots, b^{n-1}$ is a basis of an A-module B and since the matrix is invertible, $1, c_1, \ldots, c_{n-1}$ is also a basis.

2. By $b \cdot (c_0 X^{n-1} + \cdots + c_{n-1}) = (c_0 X^{n-1} + \cdots + c_{n-1})X - P$, we have

$$b \begin{pmatrix} 1 \\ c_1 \\ \vdots \\ c_{n-1} \end{pmatrix} = \begin{pmatrix} -a_1 & 1 & & 0 \\ -a_2 & 0 & \ddots & \\ \vdots & \vdots & \ddots & 1 \\ -a_n & 0 & \cdots & 0 \end{pmatrix} \begin{pmatrix} 1 \\ c_1 \\ \vdots \\ c_{n-1} \end{pmatrix} \quad \text{and} \quad b \begin{pmatrix} 1 \\ f_1 \\ \vdots \\ f_{n-1} \end{pmatrix} = \begin{pmatrix} -a_1 & -a_2 & \cdots & -a_n \\ 1 & 0 & \cdots & 0 \\ & \ddots & \ddots & \vdots \\ 0 & & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ f_1 \\ \vdots \\ f_{n-1} \end{pmatrix} \tag{1.2}$$

The second equality means that $f_i = b^{n-1-i} f_{n-1}$ for $i = 0, \ldots, n-1$ and that f_{n-1} defines an isomorphism $B = A[X]/(P) \to \mathrm{Hom}_A(B, A)$ of B-modules.

3. By (1.1) and 2, we have

$$\begin{pmatrix} g_0 \\ g_1 \\ \vdots \\ g_{n-1} \end{pmatrix} = \begin{pmatrix} 1 & a_1 & \cdots & a_n \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & a_1 \\ 0 & \cdots & 0 & 1 \end{pmatrix} \begin{pmatrix} f_0 \\ f_1 \\ \vdots \\ f_{n-1} \end{pmatrix} = \begin{pmatrix} 1 & a_1 & \cdots & a_n \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & a_1 \\ 0 & \cdots & 0 & 1 \end{pmatrix} \begin{pmatrix} b^{n-1} \\ b^{n-2} \\ \vdots \\ 1 \end{pmatrix} f_{n-1} = \begin{pmatrix} c_{n-1} \\ c_{n-2} \\ \vdots \\ 1 \end{pmatrix} f_{n-1}. \tag{1.3}$$

□

We express the trace mapping using the basis in Lemma 1.2.1.

Proposition 1.2.2. *Let A be a ring and let $P \in A[X]$ be a monic polynomial. Let $b \in B = A[X]/(P)$ be the image of $X \in A[X]$ and let $f_{n-1} = g_{n-1}$ be the basis of the free B-module $\mathrm{Hom}_A(B, A)$ of rank 1 constructed in Lemma 1.2.1. Then, we have*

$$\mathrm{Tr}_{B/A} = P'(b) \cdot f_{n-1}$$

in $\mathrm{Hom}_A(B, A)$. In particular, if B is étale over A, we have

$$\mathrm{Tr}_{B/A} \frac{b^i}{P'(b)} = \begin{cases} 1 & \text{if } i = n-1, \\ 0 & \text{if } i = 0, \dots, n-2. \end{cases} \tag{1.4}$$

Proof. If $x_1, \dots, x_n$ is a basis of the free A-module B and $f_1, \dots, f_n \in \mathrm{Hom}_A(B, A)$ is the dual basis, for $x \in B$, we have $\mathrm{Tr}_{B/A} x = \sum_i f_i(xx_i) = \sum_i x_i f_i(x)$ and we have $\mathrm{Tr}_{B/A} = \sum_i x_i f_i \in \mathrm{Hom}_A(B, A)$. Applying this to the basis $1, \dots, b^{n-1}$ and in the notation of Lemma 1.2.1, we obtain

$$\mathrm{Tr}_{B/A} = \sum_{i=0}^{n-1} b^i g_i = \sum_{i=0}^{n-1} c_{n-1-i} b^i f_{n-1} = Q(b) \cdot f_{n-1}$$

for $Q = c_0 X^{n-1} + \cdots + c_{n-1} \in B[X]$ by Lemma 1.2.1.3. By $P = (X - b) \cdot Q$, we have $P' = Q + (X - b)Q'$ and $\mathrm{Tr}_{B/A} = Q(b) \cdot f_{n-1} = P'(b) \cdot f_{n-1}$.

If B is étale, then $P'(b)$ is invertible and we have $g_{n-1} = f_{n-1} = 1/P'(b) \cdot \mathrm{Tr}_{B/A}$ by Lemma 1.2.1.3. This means (1.4). □

As an application of Proposition 1.2.2, we show that rings étale over normal rings are again normal.

Proposition 1.2.3. *Let A be a ring and $P \in A[X]$ be a monic polynomial. Set $B = A[X]/(P)$ and let $b \in B$ be the image of X. If A is normal, then $B' = B[P'(b)^{-1}]$ is also normal.*

Proof. By replacing A by the local ring at any prime ideal, we may assume that A is an integrally closed integral domain. Let K be the fraction field of A and set $L = B \otimes_A K$ and $L' = B' \otimes_A K$. Since B' is flat over A, the morphism $B' \to L'$ is an injection. First, we reduce it to the case where the surjection $L \to L'$ is an isomorphism.

Since A is integrally closed, the minimal polynomial $Q \in K[X]$ of the image $b_1 \in L'$ of b is contained in $A[X]$. The image $B_1 \subset L'$ of B is identified with the quotient ring $A[X]/(Q)$ of $B = A[X]/(P)$ since Q divides P. Since the surjection $B \to B_1$ induces a surjection $B' \to B_1[P'(b_1)^{-1}]$ of subrings of L', we may identify $B' = B_1[P'(b_1)^{-1}]$. If we define $R \in A[X]$ by $P = QR$, then we have $P'(b_1) = Q'(b_1)R(b_1)$. Hence $B' = B_1[P'(b_1)^{-1}]$ is a localization of $B_1[Q'(b_1)^{-1}]$. Thus by replacing P by Q, we may assume $L = L'$.

Since $L = B' \otimes_A K$ is étale over K by Lemma 1.1.5, the ring L is a product of finitely many finite separable extensions of K by Proposition 1.1.7.2 (1)⇒(2). Let $C \subset L$ be the normalization of B. Since A is normal, we have $\mathrm{Tr}_{L/K} C \subset A$. Hence the injection $\mathrm{Tr}_{B/A} \colon B \to \mathrm{Hom}_A(B, A)$ is extended to an injection $C \to \mathrm{Hom}_A(B, A)$. Thus we obtain injections $B' = B[P'(b)^{-1}] \to C[P'(b)^{-1}] \to \mathrm{Hom}_A(B, A) \otimes_B B[P'(b)^{-1}]$. Since the composition is an isomorphism by Proposition 1.2.2, the first morphism $B' \to C[P'(b)^{-1}]$ is an isomorphism and B' is normal. □

Corollary 1.2.4. *Let B be a ring étale over A.*

1. *If A is normal, then B is also normal.*

2. *If A is a discrete valuation ring with the maximal ideal $\mathfrak{m}$ and if $\mathfrak{n} \subset B$ is a prime ideal such that the inverse image is $\mathfrak{m} \subset A$ of A, then the local ring $B_{\mathfrak{n}}$ is a discrete valuation ring.*

Proof. 1. By Theorem 1.1.9, we may assume that $B = A[X]/(P)[P'^{-1}]$ for a monic polynomial $P \in A[X]$. Hence the assertion follows from Proposition 1.2.3.

2. By 1, $B_{\mathfrak{n}}$ is a normal local noetherian ring. Since $B_{\mathfrak{n}}$ has exactly two prime ideals, the maximal ideal $\mathfrak{n}B_{\mathfrak{n}}$ and 0, it follows that $B_{\mathfrak{n}}$ is a discrete valuation ring. □

Exercise 1.2. Let the notation be as in Lemma 1.2.1. Compute $\mathrm{Tr}_{B/A} c_i$ for $i = 0, \ldots, n-1$. Let $\boldsymbol{A}$ denote the matrix in (1.1) and show $\begin{pmatrix} \mathrm{Tr}_{B/A}\, 1 \\ \mathrm{Tr}_{B/A}\, b \\ \vdots \\ \mathrm{Tr}_{B/A}\, b^{n-1} \end{pmatrix} = \boldsymbol{A}^{-1} \begin{pmatrix} n \\ (n-1)a_1 \\ \vdots \\ a_{n-1} \end{pmatrix}$.

Solution. We have $\mathrm{Tr}_{B/A} = P'(b) \cdot f_{n-1} = n \cdot f_0 + (n-1)a_1 \cdot f_1 + \cdots + a_{n-1} \cdot f_{n-1}$ by Proposition 1.2.2 and Lemma 1.2.1.2. Hence $\mathrm{Tr}_{B/A} c_i = (n-i)a_i$ for $i = 0, \ldots, n-1$. By (1.1), we have $\begin{pmatrix} 1 \\ b \\ \vdots \\ b^{n-1} \end{pmatrix} = \boldsymbol{A}^{-1} \begin{pmatrix} 1 \\ c_1 \\ \vdots \\ c_{n-1} \end{pmatrix}$. By applying $\mathrm{Tr}_{B/A}$ on the both sides, we obtain the equality.

1.3 Henselian local rings

If you are interested only in complete discrete valuation rings, you may skip this section and read henselian as complete in the later sections admitting the characterization of henselian discrete valuation rings Proposition 1.4.4 and Hensel's lemma Lemma 1.4.6. Henselian local rings are defined as follows.

Definition 1.3.1. *Let A be a local ring and $\mathfrak{m}$ be the maximal ideal.*

1. *We say that a ring B over A is an étale neighborhood of $\mathfrak{m}$ if a morphism $B \to A/\mathfrak{m}$ over A is given and if B is étale over A.*

2. *We say that A is henselian if for any étale neighborhood B of $\mathfrak{m}$ and $\mathfrak{n} = \mathrm{Ker}(B \to A/\mathfrak{m})$, the morphism $A \to B_{\mathfrak{n}}$ to the localization is an isomorphism.*

A field is a henselian local ring as we will see in Corollary 1.3.3 below.

Proposition 1.3.2 ([54, Chapitre 7, §3, Proposition 3])**.** *Let A be a local ring and $F = A/\mathfrak{m}$ be the residue field. Then, the following conditions are equivalent:*

(1) *A is henselian.*

(2) *Let $P \in A[X]$ be a polynomial and let $\overline{a} \in F$ be a root of $\overline{P} \in F[X]$ satisfying $\overline{P}'(\overline{a}) \neq 0$. Then, there exists a root $a \in A$ of P satisfying $a \equiv \overline{a} \bmod \mathfrak{m}$.*

(2′) *Let $P \in A[X]$ be a monic polynomial and let $\overline{a} \in F$ be a simple root of $\overline{P} \in F[X]$. Then, there exists a root $a \in A$ of P satisfying $a \equiv \overline{a} \bmod \mathfrak{m}$.*

In conditions (2) and (2′), the solution a congruent to $\overline{a}$ is unique.

Proof. 1. (1)⇒(2): The ring $B = A[X]/(P)[P'^{-1}]$ is étale over A by Lemma 1.1.5. Hence B is an étale neighborhood of $\mathfrak{m}$ with respect to the surjection $B \to F$ defined by the solution $\overline{a}$ of $\overline{P}$. Since A is henselian, the morphism $A \to B_{\mathfrak{n}}$ to the localization at $\mathfrak{n} = \mathrm{Ker}(B \to F)$ is an isomorphism. The composition $B \to B_{\mathfrak{n}} \to A$ with its inverse defines a unique root a of P lifting $\overline{a}$.

(2)⇒(2′): If $\overline{a}$ is a simple root of $\overline{P}$, we have $\overline{P}'(\overline{a}) \neq 0$.

(2′)⇒(1): Let B be an étale neighborhood of $\mathfrak{m}$ and $\mathfrak{n} = \mathrm{Ker}(B \to F)$. By Theorem 1.1.9 (1)⇒(2), we may assume that $B = A[X]/(P)[P'^{-1}]$ for a monic polynomial $P \in A[X]$. Let $\overline{a} \in F$ be the image of X by $B \to F$. Then, $\overline{P}'(\overline{a}) \neq 0$ and the morphism $B/\mathfrak{n} \to F$ defined by $\overline{a}$ is lifted to a section $B \to A$ defined by a lifting a of $\overline{a}$ by (2′). This induces an isomorphism $B_{\mathfrak{n}} \to A$ by Lemma 1.1.6.2. □

A complete noetherian local ring is a henselian local ring.

Corollary 1.3.3. *Let $A = \varprojlim_n A/\mathfrak{m}^n$ be a complete noetherian local ring. Then A is henselian. In particular a field is a henselian local ring. In other words, a complete noetherian local ring A satisfies* (2) *in Proposition* 1.3.2.

The last property in Corollary 1.3.3 is called Hensel's lemma.

Proof. We show that A satisfies the condition (2) in Proposition 1.3.2. The case where A is a field is clear. Let $\mathfrak{m} \subset A$ be the maximal ideal. Since $B = A[X]/(P)[P'^{-1}]$ is étale over A by Lemma 1.1.5, the mapping $\mathrm{Mor}_A(B, A/\mathfrak{m}^{n+1}) \to \mathrm{Mor}_A(B, A/\mathfrak{m}^n)$ is a bijection for every $n \geqq 1$ by Theorem 1.1.10. Hence by induction on n, there exists a unique solution $a_n \in A/\mathfrak{m}^n$ of $P = 0$ satisfying $a_n \bmod \overline{a} \bmod \mathfrak{m}$. Then $a = (a_n)_n \in A = \varprojlim A/\mathfrak{m}^n$ is a solution of $P = 0$. □

We give another criterion for a local ring to be henselian.

Proposition 1.3.4 ([54, Chapitre 7, §3, Proposition 3])**.** *Let A be a local ring and $F = A/\mathfrak{m}$ be the residue field. Then, the following conditions are equivalent:*

(1) *A is henselian.*

(2) *Let B be a ring finite over A. Then, B is isomorphic to a finite product $\prod_{i \in I} B_i$ of local rings.*

Proof. (1)⇒(2): First, we show that a field $A = K$ satisfies the condition (2). Let B be a ring over K of finite dimension as a K-vector space. We prove that the condition (2) is satisfied by induction on the dimension $\dim_K B$. If $\dim = 0$, then $B = 0$. Assume $B \neq 0$ and let $\mathfrak{m} \subset B$ be a maximal ideal. Then, there exists an integer $n \geqq 1$ such that $\mathfrak{m}^{n+1} = \mathfrak{m}^n$. By Lemma 1.1.6.1, B is decomposed as a product $B = B/\mathfrak{m}^n \times B'$. Since $B/\mathfrak{m}^n$ is a local ring and $\dim_K B' < \dim_K B$, the assertion follows.

Assume that A is henselian and let $\mathfrak{m}$ be the maximal ideal. Let B be a ring finite over A. First assume that B is free of finite rank as an A-module. Let F be the functor in Lemma 1.1.5.2 for B over A and let E be the ring étale over A representing F. Since $B/\mathfrak{m}B$ is of finite dimension over $A/\mathfrak{m}$, it isomorphic to a product $\prod_i (B/\mathfrak{m}B)_i$ of finitely many local rings. Let $e_i \in B/\mathfrak{m}B$ be the corresponding primitive idempotents. Then each $e_i \in \mathrm{Idem}\, B/\mathfrak{m}B = F(A/\mathfrak{m})$ defines a morphism $E \to A/\mathfrak{m}$ over A.

Since E is étale over A, the ring E is an étale neighborhood of $\mathfrak{m}$ with respect to the morphism $E \to A/\mathfrak{m}$ corresponding to e_i. Since A is henselian, for the kernel $\mathfrak{n}_i = \mathrm{Ker}(E \to A/\mathfrak{m})$, the morphism $A \to E_{\mathfrak{n}_i}$ is an isomorphism and the corresponding morphism $E \to E_{\mathfrak{n}_i} \to A$ defines an idempotent $\widetilde{e}_i \in F(A) = \mathrm{Idem}\, B$ lifting e_i. Then,

the product $B \to \prod_i B_i$ of the projections $B \to B_i = B/(1-\widetilde{e}_i)$ is an isomorphism by Nakayama's lemma. Since $B_i/\mathfrak{m}B_i = (B/\mathfrak{m}B)_i$ is a local ring, B_i is also a local ring.

We show the general case. Let $b_1, \ldots, b_n$ be a system of generators of B over A and let $P_1, \ldots, P_n \in A[X]$ be monic polynomials satisfying $P_i(b_i) = 0$. Then, $B' = A[X_1, \ldots, X_n]/(P_1(X_1), \ldots, P_n(X_n))$ is free of finite rank as an A-module and the morphism $B' \to B$ over A sending X_i to b_i is a surjection. Since B' is already shown to be a product of finitely many local rings, its quotient B is also a product of finitely many local rings.

(2)⇒(1): We show that the condition (2′) in Proposition 1.3.2 is satisfied. If $P \in A[X]$ is a monic polynomial, then $B = A[X]/(P)$ is a free A-module. If $\overline{a} \in F$ is a simple root of $\overline{P}$, then $\overline{B} = F[X]/(\overline{P})$ is isomorphic to a product $F \times \overline{B}_1$. If B is a product of local rings, we have $B = B_0 \times B_1$ such that $B_0 \otimes_A F = F$. Since B_0 is a free A-module, the canonical morphism $A \to B_0$ is an isomorphism by Nakayama's lemma. □

Proposition 1.3.5 ([54, Chapitre 8, Théorème 1])**.** *The inclusion*

$$\text{(henselian local rings)} \to \text{(local rings)} \tag{1.5}$$

of a full subcategory has a left adjoint. If A^{h} denotes the image of a local ring A by the adjoint functor, the canonical morphism $A \to A^{\mathrm{h}}$ is faithfully flat and induces an isomorphism on the residue fields.

For a local ring A, we call its image by the adjoint functor of (1.5) the henselization of A and write it by A^{h}.

Proof. Let A be a local ring and F be the residue field. Let $(A \to A_i \to F)_{i\in I}$ be a cofinal filtered system of étale neighborhoods of the maximal ideal $\mathfrak{m}$ of A and set $\widetilde{A} = \varinjlim_{i\in I} A_i$. Since A_i are flat over A, the local morphism $A \to \widetilde{A}$ is faithfully flat. We show that the local ring $\widetilde{A}$ is henselian. Let $\widetilde{B}$ be an étale neighborhood of the maximal ideal $\widetilde{\mathfrak{m}}$ of $\widetilde{A}$ and let $\widetilde{\mathfrak{n}} \subset \widetilde{B}$ be the kernel of $\widetilde{B} \to \widetilde{A}/\widetilde{\mathfrak{m}} = F$. Then, since $\widetilde{B}$ is of finite presentation over $\widetilde{A}$, there exist $i \in I$, a ring B_i étale over A_i and an isomorphism $B_i \otimes_{A_i} \widetilde{A} \to \widetilde{B}$. Since B_i is an étale neighborhood of $\mathfrak{m}$ and since $(A_i)_{i\in I}$ is cofinal, there exist $j \geqq i$ and an morphism $B_i \to A_j$. This induces a morphism $\widetilde{B} \to \widetilde{A}$ and an isomorphism $\widetilde{A} \to \widetilde{B}_{\widetilde{\mathfrak{n}}}$ by Lemma 1.1.6.2.

Let B be a henselian local ring with maximal ideal $\mathfrak{n}$ and let $A \to B$ be a local morphism. We show that there exists a unique local morphism $\widetilde{A} \to B$ compatible with $A \to B$. Let $i \in I$. Then, $B_i = A_i \otimes_A B$ is étale over B and the kernel of $A_i \to F$ defines a maximal ideal $\mathfrak{n}_i$ of B_i such that $B/\mathfrak{n} \to B_i/\mathfrak{n}_i$ is an isomorphism. Since B is henselian, the morphism $B \to B_{i,\mathfrak{n}_i}$ to the localization is an isomorphism. The compositions $A_i \to B_{i,\mathfrak{n}_i} \to B$ with its inverse define an inductive system of morphisms and $\widetilde{A} \to B$. The uniqueness follows from the construction.

Since the residue field F is henselian, the local morphism $A \to F$ defines a morphism $A^{\mathrm{h}} \to F^{\mathrm{h}} = F$ compatible with $A \to A^{\mathrm{h}}$. □

Corollary 1.3.6. *Let $A \to B$ be a finite morphism of local rings.*

1. *If A is a henselian local ring, then B is also a henselian local ring.*
2. *Let A^{h} and B^{h} be the henselizations. Then, the morphism $B \otimes_A A^{\mathrm{h}} \to B^{\mathrm{h}}$ is an isomorphism.*

Proof. 1. Let C be a ring finite over B. Then, since C is finite over A, the ring C is a product of local rings by Proposition 1.3.4 (1)⇒(2). Hence B is henselian by Proposition 1.3.4 (2)⇒(1).

2. Since the ring $B \otimes_A A^{\mathrm{h}}$ finite over A^{h} has a unique prime ideal above the maximal ideal of A^{h}, it is a local ring and hence is henselian by 1. By the universality of B^{h}, we obtain a morphism $B^{\mathrm{h}} \to B \otimes_A A^{\mathrm{h}}$ going the other way. By the universality of the henselizations and the tensor product, they are inverse to each other. □

Exercise 1.3. Show that the field $\mathbf{Q}_p$ of p-adic numbers contains all the $p-1$-st roots of 1.

Solution. Since $\mathbf{Q}_p$ is complete, $\mathbf{Z}_p$ is a henselian local ring by Corollary 1.3.3. The polynomial $X^{p-1} - 1 \in \mathbf{Z}_p[X]$ is decomposed as $X^{p-1} - 1 = \prod_{a \in \mathbf{F}_p^\times}(X - a)$ in $\mathbf{F}_p[X]$. Hence we may apply Proposition 1.3.2 (2′).

1.4 Finite extensions

We study elementary properties of finite extensions of henselian discrete valuation fields.

Definition 1.4.1. *We call the fraction field K of a discrete valuation ring $\mathcal{O}_K$ a discrete valuation field.*

Let K and L be discrete valuation field and $K \to L$ be a morphism of fields. If $K \to L$ induces a local morphism $\mathcal{O}_K \to \mathcal{O}_L$ of discrete valuation rings, we say that L is an extension of discrete valuation field K.

If L is an extension of discrete valuation field K, the ramification index $e_{L/K}$ is the unique integer $e \geqq 1$ satisfying $\mathfrak{m}_L^e = \mathfrak{m}_K \mathcal{O}_L$ for the maximal ideals $\mathfrak{m}_K \subset \mathcal{O}_K$ and $\mathfrak{m}_L \subset \mathcal{O}_L$.

We say that a finite extension L is a totally ramified extension of K if the normalization $\mathcal{O}_L$ is a discrete valuation ring, if the morphism $\mathcal{O}_K/\mathfrak{m}_K \to \mathcal{O}_L/\mathfrak{m}_L$ of residue fields is an isomorphism and if $e_{L/K} = [L : K]$.

If $\mathcal{O}_K$ is henselian (resp. complete), we call K a henselian (resp. complete) discrete valuation field.

The residue field $\mathcal{O}_K/\mathfrak{m}_K$ of a discrete valuation ring $\mathcal{O}_K$ will be denoted by F. By Corollary 1.3.3, a complete discrete valuation field is a henselian discrete valuation field.

Proposition 1.4.2. *Let K be a discrete valuation field with residue field F. Let L be a finite extension of K and assume that the integral closure $\mathcal{O}_L$ of $\mathcal{O}_K$ is a discrete valuation ring. Then, the residue field E of L is a finite extension of F and the dimension of the F-vector space $\mathcal{O}_L/\mathfrak{m}_K\mathcal{O}_L$ is $e_{L/K} \cdot [E : F] \leqq [L : K]$. If $\mathcal{O}_L$ is finite over $\mathcal{O}_K$, then the equality $e_{L/K} \cdot [E : F] = [L : K]$ holds.*

Proof. Let E be the residue field of L. The F-vector space $\mathcal{O}_L/\mathfrak{m}_K\mathcal{O}_L$ is a successive extension of $\mathfrak{m}_L^i/\mathfrak{m}_L^{i+1}$ for $i = 0, \ldots, e-1$. If $x_1, \ldots, x_n \in \mathcal{O}_L$ are liftings of elements of E linearly independent over F and if t is a uniformizer of L, then the images of $x_i t^j; i = 1, \ldots, n, j = 0, \ldots, e-1$ form a basis of an F-vector space of $\mathcal{O}_L/\mathfrak{m}_K\mathcal{O}_L$ and the submodule $\langle x_i t^j; i = 1, \ldots, n, j = 0, \ldots, e-1\rangle \subset \mathcal{O}_L$ is a free $\mathcal{O}_K$-module of rank $n \cdot e \leqq [L : K]$. Hence E is a finite extension of F and we have $[E : F] \cdot e_{L/K} \leqq [L : K]$.

If the torsion free $\mathcal{O}_K$-module $\mathcal{O}_L$ is of finite type, it is a free module and its rank $[L : K]$ equals the dimension $[E : F] \cdot e_{L/K}$ of the F-vector space $\mathcal{O}_L/\mathfrak{m}_K\mathcal{O}_L$. □

Totally ramified extensions are generated by roots of Eisenstein polynomials. We say that a monic polynomial $P \in \mathcal{O}_K[X]$ of degree n is an Eisenstein polynomial if $P \equiv X^n \bmod \mathfrak{m}_K$ and if the constant term $t = P(0)$ is a uniformizer of K.

Lemma 1.4.3. *Let K be a discrete valuation field.*

1. *Let $P \in \mathcal{O}_K[X]$ be an Eisenstein polynomial. Then, $L = K[X]/(P)$ is a totally ramified extension of K, the integral closure $\mathcal{O}_L$ is $\mathcal{O}_K[X]/(P)$ and the class x of X is a uniformizer.*

2. *Conversely, let L be a totally ramified extension of K and x be a uniformizer of $\mathcal{O}_L$. Then, the minimal polynomial $P \in \mathcal{O}_K[X]$ of x is an Eisenstein polynomial and $\mathcal{O}_L = \mathcal{O}_K[x]$.*

Proof. 1. Let $B = \mathcal{O}_K[X]/(P)$. Then, $v(\sum_{i=0}^{n-1} a_i x^i) = \min_i(i + n \cdot \mathrm{ord}_K a_i)$ defines a discrete valuation and B is a discrete valuation ring with uniformizer x. Hence L is a totally ramified extension and B is the integral closure.

2. We have $\mathcal{O}_L/\mathfrak{m}_K\mathcal{O}_L = F[x]/(x^n)$. Hence we have $\deg P = [L : K] = n$ and $P \equiv X^n \bmod \mathfrak{m}_K$. The constant term $t = P(0)$ equals $x^n u \in \mathcal{O}_K$ for a unit $u \in \mathcal{O}_L^\times$ and is a uniformizer of K since $e_{L/K} = n$. Hence P is an Eisenstein polynomial and the subring $\mathcal{O}_K[x]$ is isomorphic to $\mathcal{O}_K[X]/(P)$ and equals $\mathcal{O}_L$ by 1. □

Proposition 1.4.4. *Let K be a discrete valuation field and $\mathcal{O}_K$ be the valuation ring. Then, the following conditions are equivalent:*

(1) *$\mathcal{O}_K$ is henselian.*

(2) *Let L be a finite separable extension of discrete valuation field K. If the ramification index $e_{L/K}$ is 1 and if the morphism $\mathcal{O}_K/\mathfrak{m}_K \to \mathcal{O}_L/\mathfrak{m}_L$ of residue fields is an isomorphism, then $K \to L$ is an isomorphism.*

(3) *Let L be a finite extension of K. Then, the integral closure $\mathcal{O}_L$ of $\mathcal{O}_K$ in L is a discrete valuation ring.*

Proof. (1)⇒(3): The integral closure $\mathcal{O}_L$ is the inductive limit $\varinjlim_\lambda B_\lambda$ of subrings finite over $\mathcal{O}_K$. Since $\mathcal{O}_K$ is henselian and since the extension L has a unique idempotent, each B_λ is local and the morphisms $B_\lambda \to B_\mu$ are local. Hence their limit $\mathcal{O}_L$ is also local.

We show that $\mathcal{O}_L$ is a discrete valuation ring. Assume first that L is a separable extension of K. Since $\mathcal{O}_K$ is noetherian, the integral closure $\mathcal{O}_L \subset L$ of $\mathcal{O}_K$ is finite over $\mathcal{O}_K$. Hence $\mathcal{O}_L$ is a normal noetherian local ring and has exactly two prime ideals 0 and the maximal ideal. Therefore $\mathcal{O}_L$ is a discrete valuation ring in this case. By replacing K by the separable closure in L, we may assume that L is a purely inseparable extension of K. Let $q = [L : K]$ be the degree of the extension. Then, since $\frac{1}{q}\mathrm{ord}_K x^q$ is the unique valuation of L extending ord_K, an element $x \in L$ is integral over $\mathcal{O}_K$ if and only if $x^q \in \mathcal{O}_K$. Hence the integral closure $\mathcal{O}_L \subset L$ of $\mathcal{O}_K$ is a discrete valuation ring.

(3)⇒(2): By (3), the normalization B of $\mathcal{O}_K$ in L is a discrete valuation ring. Hence the subring $B \subset \mathcal{O}_L$ equals $\mathcal{O}_L$. Since L is a finite separable extension, $B = \mathcal{O}_L$ is finite over $\mathcal{O}_K$. Hence the morphism $\mathcal{O}_K \to \mathcal{O}_L$ is an isomorphism by Nakayama's lemma.

(2)⇒(1): Let B be a ring étale over $\mathcal{O}_K$ and $\mathfrak{n} \subset B$ be the maximal ideal such that $F = \mathcal{O}_K/\mathfrak{m}_K \to B/\mathfrak{n}$ is an isomorphism. Then, the local ring $B_\mathfrak{n}$ is a discrete valuation ring by Corollary 1.2.4.2 and its fraction field L is a finite separable extension of K by Proposition 1.1.7.1 (1)⇒(2). Since $e_{L/K} = 1$ and $F \to B/\mathfrak{n}$ is an isomorphism, the morphisms $K \to L$ and $\mathcal{O}_K \to B_\mathfrak{n}$ are isomorphism by (2). □

Corollary 1.4.5. *Let K be a discrete valuation field with residue field F. Let L be a finite extension of K and $\mathcal{O}_L$ be the integral closure of $\mathcal{O}_K$.*

1. *If K is henselian, then $\mathcal{O}_L$ is a henselian discrete valuation ring.*
2. *If K is complete, then $\mathcal{O}_L$ is finite over $\mathcal{O}_K$ and L is also complete.*

Proof. 1. By Proposition 1.4.4 (1)⇒(3), the integral closure $\mathcal{O}_L \subset L$ of $\mathcal{O}_K$ is a discrete valuation ring. We may write the local ring $\mathcal{O}_L$ as an inductive limit $\varinjlim_i B_i$ of finite local rings B_i with the same residue fields as $\mathcal{O}_L$. By Corollary 1.3.6, B_i are henselian. Hence the inductive limit $\mathcal{O}_L$ is also henselian by Proposition 1.3.2 (1)⇔(2′).

2. By Corollary 1.3.3, K is henselian and by 1, $\mathcal{O}_L$ is a discrete valuation ring. Since $\mathcal{O}_L/\mathfrak{m}_K\mathcal{O}_L$ is of finite dimension by Proposition 1.4.2, there exists a finitely many elements in $\mathcal{O}_L$ generating the completion $\mathcal{O}_{\widehat{L}} = \varprojlim_n \mathcal{O}_L/\mathfrak{m}_K^n\mathcal{O}_L$ as an $\mathcal{O}_K$-module by Nakayama's lemma. Hence the injection $\mathcal{O}_L \to \mathcal{O}_{\widehat{L}}$ is an isomorphism of $\mathcal{O}_K$-modules of finite type. □

For henselian discrete valuation rings, we will use Proposition 1.3.2 (2) in the following generalized form. We will refer to this as Hensel's lemma.

Lemma 1.4.6. *Let K be a henselian discrete valuation field and $P \in \mathcal{O}_K[X]$ be a polynomial. Let $a \in \mathcal{O}_K$ and assume $P'(a) \neq 0$ and $\mathrm{ord}_K P(a) > 2 \cdot \mathrm{ord}_K P'(a)$. Let $n = \mathrm{ord}_K P'(a) < m$ be integers satisfying $n + m \leqq \mathrm{ord}_K P(a)$. Then, there exists a unique solution $x \in \mathcal{O}_K$ of $P(x) = 0$ satisfying $x \equiv a \bmod \mathfrak{m}_K^m$.*

Proof. Let t be a generator of $\mathfrak{m}_K^{m-1}$. Since $P(a + tX) \equiv P(a) + P'(a)tX \bmod t^2$ and $P'(a)t$ divides $P(a)$ and t^2, we have $Q(X) = P(a + tX)/P'(a)t \in \mathcal{O}_K[X]$. Since $Q(0) \equiv P(a)/P'(a)t \equiv 0 \bmod \mathfrak{m}_K$ and $Q'(0) \equiv 1 \bmod \mathfrak{m}_K$, there exists a unique solution $x \in \mathfrak{m}_K$ of $Q(x) = 0$ by Proposition 1.3.2 (1)⇒(2). This means that there exists a unique solution $x \equiv a \bmod \mathfrak{m}_K^m$ of $P(x) = 0$. □

The henselization and the completion have the same absolute Galois groups.

Proposition 1.4.7 ([7, Lemme 2.2.1])**.** *Let K be a henselian discrete valuation field and let $\widehat{K}$ be the completion of K. Then, the completion defines an equivalence of categories*

$$\text{(Finite separable extensions of } K) \to \text{(Finite separable extensions of } \widehat{K}). \tag{1.6}$$

For any finite separable extension L over K, the canonical morphism

$$\mathcal{O}_L \otimes_{\mathcal{O}_K} \mathcal{O}_{\widehat{K}} \to \mathcal{O}_{\widehat{L}} \tag{1.7}$$

is an isomorphism.

Proof. Let L be a finite separable extension of K. By Proposition 1.4.4 and Corollary 1.4.5.2, the normalization $\mathcal{O}_L$ is a discrete valuation ring and the tensor product $\mathcal{O}_L \otimes_{\mathcal{O}_K} \mathcal{O}_{\widehat{K}}$ is the completion of $\mathcal{O}_L$ and hence is a discrete valuation ring. Consequently, $L \otimes_K \widehat{K}$ is the completion $\widehat{L}$ of L and is a finite separable extension of $\widehat{K}$. Thus the morphism $G_{\widehat{K}} \to G_K$ of absolute Galois groups is a surjection.

To prove the injectivity of $G_{\widehat{K}} \to G_K$, it suffices to show the essential surjectivity of the functor (1.6). Namely, we show that for any finite separable extension M of $\widehat{K}$, there exist a finite separable extension L of K and an isomorphism $L \otimes_K \widehat{K} \to M$. Take an element $a \in \mathcal{O}_M$ such that $M = \widehat{K}(a)$ and let $P \in \mathcal{O}_{\widehat{K}}[X]$ be the minimal polynomial.

Since M is a separable extension, we have $P'(a) \neq 0$. Let $m > n = \mathrm{ord}_M P'(a)$ be an integer such that $\mathfrak{m}_M^m \subset \mathfrak{m}_K \cdot \mathcal{O}_{\widehat{K}}[a] \subset \mathcal{O}_M$.

Take a monic polynomial $Q \in \mathcal{O}_K[X]$ such that $Q \equiv P \bmod \mathfrak{m}_K^{n+m}$. We have $Q(a) \equiv P(a) = 0 \bmod \mathfrak{m}_M^{n+m}$. Since $Q'(a) \equiv P'(a) \bmod \mathfrak{m}_M^{n+m}$, we have $\mathrm{ord}_M Q'(a) = \mathrm{ord}_M P'(a)$. Hence by Hensel's lemma, there exists a unique solution $b \equiv a \bmod \mathfrak{m}_M^m$ of $Q(b) = 0$. Since $b \in a + \mathfrak{m}_M^m \subset \mathcal{O}_{\widehat{K}}[a]$, the solution b of Q defines a morphism $\mathcal{O}_{\widehat{K}}[X]/(Q) \to \mathcal{O}_{\widehat{K}}[a]$ over $\mathcal{O}_{\widehat{K}}$. Since this is a morphism of $\mathcal{O}_{\widehat{K}}$-modules of the same rank and $b \equiv a \bmod \mathfrak{m}_M^m \subset \mathfrak{m}_K \mathcal{O}_{\widehat{K}}[a]$, it is an isomorphism by Nakayama's lemma. If we set $L = K[X]/(Q)$, we obtain an isomorphism $L \otimes_K \widehat{K} \to M$. Hence L is a finite separable extension of K satisfying the required condition. □

The henselization and the completion are related as follows.

Proposition 1.4.8. *Let K be a discrete valuation field and let $\mathcal{O}_K^{\mathrm{h}}$ be the henselization of $\mathcal{O}_K$.*

1. *The henselization $\mathcal{O}_K^{\mathrm{h}}$ is a discrete valuation ring and the canonical morphism $\mathcal{O}_K \to \mathcal{O}_K^{\mathrm{h}}$ induces an isomorphism on the completions.*

2. *We identify the fraction field K^{h} of $\mathcal{O}_K^{\mathrm{h}}$ as a subfield of the completion $\widehat{K}$ by the isomorphism in* 1. *Then, we have $K^{\mathrm{h}} = \{x \in \widehat{K} \mid x \text{ is separably algebraic over } K\}$.*

Proof. 1. Write $\mathcal{O}_K^{\mathrm{h}} = \varinjlim_{i \in I} B_i$ as an inductive limit of étale neighborhoods of the maximal ideal $\mathfrak{m} \subset \mathcal{O}_K$. Let $\mathfrak{n}_i \subset B_i$ be the kernel of the surjection $B_i \to F = \mathcal{O}_K/\mathfrak{m}$. The local ring $B_{i,\mathfrak{n}_i}$ is a discrete valuation ring by Corollary 1.2.4.2 and the ramification index over $\mathcal{O}_K$ is 1 by Proposition 1.1.7.1 (1)⇒(2). Hence the limit $\mathcal{O}_K^{\mathrm{h}} = \varinjlim_{i \in I} B_{i,\mathfrak{n}_i}$ is also a discrete valuation ring of ramification index 1 over $\mathcal{O}_K$. Since the residue field of $\mathcal{O}_K^{\mathrm{h}}$ is F by Proposition 1.3.5, the morphism $\mathcal{O}_K/\mathfrak{m}_K^n \to \mathcal{O}_K^{\mathrm{h}}/\mathfrak{m}_{K^{\mathrm{h}}}^n$ is an isomorphism for every integer $n \geqq 1$ and the morphism $\widehat{\mathcal{O}}_K = \varprojlim_n \mathcal{O}_K/\mathfrak{m}_K^n \to \varprojlim_n \mathcal{O}_K^{\mathrm{h}}/\mathfrak{m}_{K^{\mathrm{h}}}^n = \widehat{\mathcal{O}}_K^{\mathrm{h}}$ of completions is an isomorphism.

2. Since K^{h} is an inductive limit of finite separable extensions of K, any element of K^{h} is separably algebraic over K. To show the other inclusion, it suffices to show that if L is a finite separable extension of K^{h} inside $\widehat{K}$, then we have $L = K^{\mathrm{h}}$. Since $\mathcal{O}_K^{\mathrm{h}} \subset \mathcal{O}_L \subset \widehat{\mathcal{O}}_K$, we have $e_{L/K^{\mathrm{h}}} = 1$ and the residue field of L is F. Hence we have $L = K^{\mathrm{h}}$ by Proposition 1.4.4 (1)⇒(2) as required. □

Exercise 1.4. Let p be a prime number and $n \geqq 1$ be an integer. Let $\zeta_{p^n} \in \mathbf{Q}_p(\zeta_{p^n})$ be a primitive p^n-th root of 1. Find the minimal polynomial of $\zeta_{p^n} - 1$ over $\mathbf{Q}_p$ and show that $\zeta_{p^n} - 1$ is a uniformizer of $\mathbf{Q}_p(\zeta_{p^n})$. Compute the degree of the extension $\mathbf{Q}_p(\zeta_{p^n})$ over $\mathbf{Q}_p$.

Solution. The cyclotomic polynomial $P = (X^{p^n} - 1)/(X^{p^{n-1}} - 1) = X^{p^{n-1}(p-1)} + \cdots + X^{p^{n-1}} + 1$ satisfies $P(X+1) \equiv X^{(p-1)p^{n-1}} \bmod p$ and $P(1) = p$. Hence $P(X+1)$ is an Eisenstein polynomial. By Lemma 1.4.3.1, $P(X+1)$ is the minimal polynomial of a uniformizer $\zeta_{p^n} - 1$ of $\mathbf{Q}_p(\zeta_{p^n})$ and $\mathbf{Q}_p(\zeta_{p^n})$ is an extension of $\mathbf{Q}_p$ of degree $(p-1)p^{n-1}$.

1.5 Tamely ramified extensions

We study finite extensions of henselian discrete valuation fields without or with little ramification.

Definition 1.5.1. *Let K be a henselian discrete valuation field and let L be a finite extension of K. Let F and E be the residue field of K and L respectively.*

1. *Assume that L is a separable extension. We say that L is an unramified extension of K if E is a separable extension of F and if $e_{L/K} = 1$. We say that L is a tamely ramified extension of K if E is a separable extension of F and if the ramification index $e_{L/K}$ is invertible in F.*

2. *If L is not a tamely ramified extension, we say that L is wildly ramified. If $E = F$, we say L is totally ramified.*

Lemma 1.5.2. *Let K be a henselian discrete valuation and let F be the residue field of K.*

1. *For any finite separable extension L of K and the integral closure $\mathcal{O}_L$ of $\mathcal{O}_K$, the following conditions are equivalent:*

(1) *$\mathcal{O}_L$ is étale over $\mathcal{O}_K$.*

(2) *L is an unramified extension of K.*

2. *Let L be an unramified extension of K. Then for any extension K' of henselian discrete valuation field K, a composition field $L' = LK'$ is an unramified extension of K'.*

Proof. 1. (1)⇒(2): By Proposition 1.1.7.2 (1)⇒(2), $\mathcal{O}_L \otimes_{\mathcal{O}_K} F$ is a finite separable extension of F. Hence L is an unramified extension of K.

(2)⇒(1): The normalization $\mathcal{O}_L$ is a free $\mathcal{O}_K$-module of finite rank. Hence $\mathcal{O}_L$ is of finite presentation and flat over $\mathcal{O}_K$. Since $\Omega^1_{\mathcal{O}_L/\mathcal{O}_K} \otimes_{\mathcal{O}_K} F = \Omega^1_{\mathcal{O}_L \otimes_{\mathcal{O}_K} F/F} = 0$, we have $\Omega^1_{\mathcal{O}_L/\mathcal{O}_K} = 0$ by Nakayama's lemma. Hence $\mathcal{O}_L$ is étale over $\mathcal{O}_K$.

2. Since $\mathcal{O}_{K'}$ is henselian, the finite ring $\mathcal{O}_L \otimes_{\mathcal{O}_K} \mathcal{O}_{K'}$ over $\mathcal{O}_{K'}$ is decomposed as a product $\prod_i B_i$ of local rings. Since $\mathcal{O}_L$ is étale over $\mathcal{O}_K$ by 1 (2)⇒(1), each B_i is étale over $\mathcal{O}_{K'}$. Hence by 1 (1)⇒(2), $L'_i = B_i \otimes_{\mathcal{O}_{K'}} K'$ is an unramified extension of K'. □

Proposition 1.5.3. *Let K be a henselian discrete valuation field and let F' be a finite separable extension of the residue field F. Then the functor* (Extensions of henselian discrete valuation field K)→(Sets) *sending L to $\mathrm{Mor}_F(F', E)$ where E denotes the residue field of L is representable by a finite unramified extension K' of K with residue field F'.*

Proof. First, we construct a finite unramified extension K' of K with residue field F'. Let $a \in F'$ be a generator over F and let $P \in \mathcal{O}_K[X]$ be a lifting as a monic polynomial of the minimal polynomial of a. Then, $\mathcal{O}_{K'} = \mathcal{O}_K[X]/(P)$ is étale over $\mathcal{O}_K$ and hence is normal by Corollary 1.2.4.1. Hence $\mathcal{O}_{K'}$ is the ring of integers in a finite separable extension K' of K and is a discrete valuation ring by Proposition 1.4.4. Therefore by Lemma 1.5.2.1 (1)⇒(2), $K' = \mathcal{O}_{K'} \otimes_{\mathcal{O}_K} K$ is a finite unramified extension of K and the residue field is F'.

We show that the canonical mapping $\mathrm{Mor}_K(K', L) \to \mathrm{Mor}_F(F', E)$ is a bijection. We may identify $\mathrm{Mor}_K(K', L) = \{x \in \mathcal{O}_L \mid P(x) = 0\}$ and $\mathrm{Mor}_F(F', E) = \{x \in E \mid \overline{P}(x) = 0\}$. Since $\overline{P} \in F[X]$ is a separable polynomial, the reduction defines a bijection $\{x \in \mathcal{O}_L \mid P(x) = 0\} \to \{x \in E \mid \overline{P}(x) = 0\}$ by Hensel's lemma. □

Corollary 1.5.4. *Let K be a henselian discrete valuation field and L be a finite extension of K.*

1. *There exists a largest subextension $M_u \subset L$ unramified over K. The residue field of M_u is the separable closure of F in E.*

2. *Let $K' \subset L$ be a subextension. Then $K'M_u$ is the largest unramified extension of K' in L.*

We call M_u the maximum unramified extension of K in L.

Proof. 1. Let F' be the separable closure of F in E. By Proposition 1.5.3, there exists an unramified extension $K' \subset L$ with residue field F'. If $K'' \subset L$ is another unramified extension with residue field $F'' \subset E$, then F'' is a subfield of F' and K'' is a subfield of K' by Proposition 1.5.3.

2. Since the residue field E of L is a purely inseparable extension of F', it is a purely inseparable extension of the residue field of $K'M_u$. Since $K'M_u$ is an unramified extension of K' by Lemma 1.5.2.2, the assertion follows. □

If the residue field F is of characteristic 0, then L is a totally and tamely ramified extension of the maximum unramified extension M_u.

Proposition 1.5.5. *Let K be a henselian discrete valuation field and let L be a finite extension of K. Assume that the residue fields F and E of K and L are of characteristic $p > 0$.*

1. *Assume that L is a tamely ramified extension of K and let K' be a extension of henselian discrete valuation K. Then, a composition field $L' = LK'$ is a tamely ramified extension of K'. The ramification index $e_{L'/K'}$ equals $e_{L/K}/\gcd(e_{L/K}, e_{K'/K})$.*

2. *Assume that E is a purely inseparable extension of F and let m be a divisor prime to p of the ramification index $e_{L/K}$. Then, there exists a unique totally ramified subextension $K' \subset L$ of degree m over K. Further, there exists a uniformizer x of K' such that x^m is a uniformizer of K.*

Proof. Existence in 2. Let $t \in K$ be a uniformizer, let $x \in L$ be an element of valuation $\mathrm{ord}_K x = 1/m$ and define a unit $u \in \mathcal{O}_L^\times$ by $t = ux^m$. By the assumption that E is a purely inseparable extension, the quotient group $E^\times/F^\times$ is p-power torsion and is an $\mathbf{Z}_{(p)}$-module. Since m is prime to p, there exist units $v \in \mathcal{O}_L^\times$ and $w \in \mathcal{O}_K^\times$ such that $u \equiv v^m/w \bmod \mathfrak{m}_L$. Since $\mathcal{O}_L$ is henselian and m is prime to p, we may assume that $u = v^m/w$ by Hensel's lemma. Hence replacing x by vx and t by wt, we may assume that $u = 1$. Then L contains an m-th root x of t and a totally ramified subextension $K[X]/(X^m - t)$ of degree m as a subfield.

1. By Proposition 1.5.3 and Corollary 1.5.4.2, after replacing K by the maximum unramified extension M_u in L and K' by $M_uK' \subset L'$, we may assume that L is a totally ramified extension of K of degree m prime to p.

First assume that $m = e_{L/K}$ divides $e_{K'/K}$. By the existence in 2 proved above, there exists a uniformizer $t \in K$ and an isomorphism $\mathcal{O}_K[X]/(X^m - t) \to \mathcal{O}_L$. By the assumption $m \mid e_{K'/K}$, there exist $y \in \mathcal{O}_{K'}$ and $v \in \mathcal{O}_{K'}^\times$ such that $t = vy^m$. Then, the normalization of $\mathcal{O}_L \otimes_{\mathcal{O}_K} \mathcal{O}_{K'} = \mathcal{O}_{K'}[X]/(X^m - vy^m)$ is a ring $\mathcal{O}_{K'}[Z]/(Z^m - v)$ étale over $\mathcal{O}_{K'}$. Since $\mathcal{O}_L[Z]/(Z^m - v)$ is further finite over $\mathcal{O}_{K'}$, the tensor product $\mathcal{O}_{K'}[Z]/(Z^m - v) \otimes_{\mathcal{O}_{K'}} K'$ is a product of finitely many unramified extensions of K' by Proposition 1.1.7.2 (1)⇒(2) and Lemma 1.5.2.1 in this case.

Thus by the decomposition $m = dm'$ where $d = (m, e_{K'/K})$, it is reduced to showing the case where m is prime to $e_{K'/K}$. Since $m = e_{L/K}$ divides $e_{L'/K} = e_{L'/K'}e_{K'/K}$ and is prime to $e_{K'/K}$, it follows that m divides $e_{L'/K'} \leqq [L' : K'] \leqq [L : K] = m$. Hence L' is a totally ramified extension of degree m of K' in this case.

Uniqueness in 2. Assume that $K'' \subset L$ is another totally ramified subextension of degree m. Then the composition $K'K'' \subset L$ is an unramified extension of K' by 1. Since E is a purely inseparable extension of F, we have $K'K'' = K'$ and the assertion follows. □

Corollary 1.5.6. *Let K be a henselian discrete valuation field and L be a finite extension of K.*

1. *There exists a largest subextension $M_t \subset L$ tamely ramified over K. The extension M_t is a totally ramified extension of the maximum unramified extension M_u and the ramification index e_{M_t/M_u} is the prime-to-p part of $e_{L/K}$.*

The degree $[L : M_t]$ is a power of p.

2. *Let $K' \subset L$ be a subextension. Then $K'M_t$ is the largest tamely ramified extension of K' in L.*

We call M_t the maximum tamely ramified extension of K in L.

Proof. 1. Let $M_u \subset L$ be the maximum unramified extension and let m be the prime-to-p part of $e_{L/K}$. By Proposition 1.5.5.2, there exists a totally ramified extension $K' \subset L$ of M_u of ramification index m. If $K'' \subset L$ is another tamely ramified extension, the composition $K'K'' \subset L$ is an unramified ramified extension of K' by Proposition 1.5.5.1. Since E is a purely inseparable extension of the residue field F' of K', we have $K'' \subset K'K'' = K'$ as in the proof of Corollary 1.5.4.1. Hence K' is the largest tamely ramified extension in L.

The ramification index of L over M_t is a power of p and the residue field E is a purely inseparable extension of the residue field of M_t. The separable closure $M_s \subset L$ of K is a finite separable extension of M_t of ramification index a power of p and the residue field extension is purely inseparable. Hence $[M_s : M_t]$ is a power of p by Proposition 1.4.2. Since L is a purely inseparable extension of M_s, the degree $[L : M_s]$ is also a power of p and the assertion follows.

2. Since the residue field E is a purely inseparable extension of F', it is a purely inseparable extension of the residue field of $K'M_t$. Further since the degree $[L : M_t]$ is a power of p, the degree $[L : K'M_t]$ is a power of p. Since $K'M_t$ is a tamely ramified extension of K' by Proposition 1.5.5.1, the assertion follows. □

Definition 1.5.7. *Let K be a henselian discrete valuation field and let L be a finite Galois extension of K of Galois group $G = \mathrm{Gal}(L/K)$. Let $M_u \subset M_t \subset L$ be the maximum unramified extension and the maximum tamely ramified extension respectively. We call the corresponding subgroups $I \supset P$ of G the inertia subgroup and the wild inertia subgroup respectively.*

Since the extensions M_u and M_t are stable under the action of G, the subgroups I and P are normal subgroups. If the residue field F is of characteristic $p > 0$, the wild inertia group P is a unique p-Sylow subgroup of I. If the residue field F is of characteristic 0, the wild inertia group P is trivial.

Proposition 1.5.8. *Let K be a henselian discrete valuation field and let L be a finite Galois extension of K of Galois group $G = \mathrm{Gal}(L/K)$. Let $I \supset P$ be the inertia subgroup and the wild inertia subgroup of G corresponding to the maximum unramified extension and the maximum tamely ramified extension $M_u \subset M_t \subset L$ respectively.*

1. *The residue field F' of M_u is a Galois extension of F and the action of G on F' defines an isomorphism $G/I \to \mathrm{Gal}(F'/F)$.*

2. *The action of I on $\mathfrak{m}_{M_t}/\mathfrak{m}_{M_t}^2$ defines an injection*

$$I/P \to F'^{\times}. \tag{1.8}$$

and the quotient I/P is a cyclic group of order $m = [M_t : M_u]$

If the residue field F is of characteristic $p > 0$, then the index $m = [I : P]$ is prime to p and the subgroup $P \subset I$ is a unique p-Sylow subgroup.

The ramification groups $G_i \subset G$ defined in the next section will be essentially a filtration on the wild inertia subgroup $P = G_1$.

Proof. 1. By Proposition 1.5.3, the canonical morphism $G/I = \mathrm{Gal}(M_u/K) \to \mathrm{Aut}_F F'$ is an isomorphism. Hence $\#\mathrm{Aut}_F F' = [F' : F]$ and F' is a Galois extension of F. Further the morphism $G/I \to \mathrm{Gal}(F'/F)$ is an isomorphism

2. Since the action of I on F' is trivial, its action on an F'-vector space $\mathfrak{m}_{M_t}/\mathfrak{m}_{M_t}^2$ of dimension 1 defines a character $I \to F'^{\times}$. By Proposition 1.5.5.2, there exist uniformizers $t \in M_u$ and $x \in M_t$ satisfying $x^m = t$. Since m is invertible in F', the reduction $\{\zeta \in M_u^{\times} \mid \zeta^m = 1\} \to \{\zeta \in F'^{\times} \mid \zeta^m = 1\}$ defines an isomorphism by Hensel's lemma. Since $M_t = M_u(x)$ is generated by an m-th root x of t, the character $I \to F'^{\times}$ induces an isomorphism $I/P = \mathrm{Gal}(M_t/M_u) \to \mu_m = \{\zeta \in F'^{\times} \mid \zeta^m = 1\}$.

The index m equals e_{M_t/M_u} and is prime to p. Since the normal subgroup $P = \mathrm{Gal}(L/M_t)$ of I is a p-group by Corollary 1.5.6 and is of index $[I : P] = m$ prime to p, it is a unique p-Sylow subgroup of I. □

For a separable closure K_s of a henselian discrete valuation field K, the maximum unramified extension and the maximum tamely ramified extension $K_u \subset K_t \subset K_s$ are defined to be the unions of finite unramified extensions and finite tamely ramified extensions.

Corollary 1.5.9. *Let K be a henselian discrete valuation field and $K_u \subset K_t \subset K_s$ be the maximum unramified extension and the maximum tamely ramified extension in a separable closure of K. Let the inertia group $I \subset G = \mathrm{Gal}(K_s/K)$ and $P \subset I$ be the corresponding subgroups. Then, the quotient G/I is identified with the absolute Galois group $\mathrm{Gal}(F_s/F)$ of the residue field F and I/P is identified with the projective limit $\varprojlim_{p \nmid m} \mu_m$. The subgroup $P \subset I$ is a unique pro-p Sylow subgroup and the quotient G/P is isomorphic to the semi-direct product $G/I \ltimes I/P$.*

Proof. By taking the limit of finite subextensions in K_s, we obtain $K_u \subset K_t \subset K_s$ and $P \subset I \subset G$. The residue field of K_u is a separable closure F_s of F by Proposition 1.5.3 and we obtain isomorphisms $G/I \to \mathrm{Gal}(K_u/K) \to \mathrm{Gal}(F_s/F) = G_F$. Since K_t is the composite extension $K_u \cdot K(s^{1/m}, p \nmid m)$ for a uniformizer $s \in K$, we obtain isomorphisms $I/P \to \mathrm{Gal}(K_t/K_u) \to \varprojlim_{p \nmid m} \mu_m$ and $G/P \to \mathrm{Gal}(K_t/K) \to \mathrm{Gal}(K_u/K) \ltimes \mathrm{Gal}(K_t/K_u) \to G_F \ltimes I/P$. Since P is a pro-p group and I/P is prime to p, P is the unique pro-p Sylow subgroup of I. □

Exercise 1.5. Let p be a prime number and $n \geqq 1$ be an integer. Assume that $n = mp^e$ is the product of an integer $m \geqq 1$ prime to p and a power $p^e > 1$ of p.

1. Find the maximum unramified extension and the maximum tamely ramified extension of $\mathbf{Q}_p$ in $\mathbf{Q}_p(\zeta_n)$.

2. Determine the Galois group $G = \mathrm{Gal}(\mathbf{Q}_p(\zeta_n)/\mathbf{Q}_p)$ and the inertia group and the wild inertia group $P \subset I \subset G$ as subgroups of $(\mathbf{Z}/n\mathbf{Z})^{\times} = (\mathbf{Z}/m\mathbf{Z})^{\times} \times (\mathbf{Z}/p^e\mathbf{Z})^{\times}$.

Solution. 1. Since $X^m - 1 \in \mathbf{F}_p[X]$ is a separable polynomial, the extension $\mathbf{Q}_p(\zeta_m)$ of $\mathbf{Q}_p$ is an unramified extension and $\mathbf{Z}_p[\zeta_m]$ is the ring of integers. Since $\mathbf{Q}_p(\zeta_{p^e})$ is a totally ramified extension of $\mathbf{Q}_p$ and $\mathbf{Z}_p[\zeta_{p^e}]$ is the ring of integers by Exercise 1.4, the morphisms $\mathbf{Q}_p(\zeta_m) \otimes_{\mathbf{Q}_p} \mathbf{Q}_p(\zeta_{p^e}) \to \mathbf{Q}_p(\zeta_n)$ and $\mathbf{Z}_p]\zeta_m] \otimes_{\mathbf{Z}_p} \mathbf{Z}_p[\zeta_{p^e}] \to \mathbf{Z}_p[\zeta_n]$ are isomorphisms. Hence

$\mathbf{Q}_p(\zeta_m) \subset \mathbf{Q}_p(\zeta_n)$ is the maximum unramified extension. Since $e_{\mathbf{Q}_p(\zeta_p)/\mathbf{Q}_p} = p-1$ is prime to p and $e_{\mathbf{Q}_p(\zeta_{p^e})/\mathbf{Q}_p}(\zeta_p) = p^{e-1}$, the composite extension $\mathbf{Q}_p(\zeta_m, \zeta_p) = \mathbf{Q}_p(\zeta_{mp})$ is the maximum tamely ramified extension.

2. By 1, we have $G = \langle p \rangle \times (\mathbf{Z}/p^e\mathbf{Z})^\times \subset (\mathbf{Z}/m\mathbf{Z})^\times \times (\mathbf{Z}/p^e\mathbf{Z})^\times$ and $I \supset P$ are identified with $(\mathbf{Z}/p^e\mathbf{Z})^\times \supset (1+p\mathbf{Z})/(1+p^e\mathbf{Z})$.

1.6 Lower ramification subgroups

We define the filtration by lower ramification groups on the Galois group of a Galois extension of henselian discrete valuation fields.

Definition 1.6.1. *Let K be a henselian discrete valuation field and let L be a finite Galois extension of K of Galois group $G = \mathrm{Gal}(L/K)$.*

1. *For an integer $i \geqq 1$, we define a normal subgroup $G_i \subset G$ by*

$$G_i = \mathrm{Ker}(G \to \mathrm{Aut}(L^\times/(1+\mathfrak{m}_L^i))) \tag{1.9}$$

and call G_i the i-th ramification group. We set G_0 to be the kernel $\mathrm{Ker}(G \to \mathrm{Aut}\, \mathcal{O}_L/\mathfrak{m}_L)$.

2. *For $\sigma \in G_0 - \{1\}$, let $i_G(\sigma)$ be the largest integer $i \geqq 0$ such that $\sigma \in G_i$. We set $i_G(1) = \infty$.*

There is another filtration called the non-logarithmic ramification groups defined by $G'_i = \mathrm{Ker}(G \to \mathrm{Aut}(\mathcal{O}_L/\mathfrak{m}_L^i))$. We compare this with that in Definition 1.6.1 in Proposition 1.6.5. For a subgroup $H \subset G$ corresponding to a subextension $M \subset L$, we have $H_i = G_i \cap H$ for every $i \geqq 0$.

Proposition 1.6.2. *Let L be a finite Galois extension of a henselian discrete valuation field K. Let F and $F' \subset E$ be the residue fields of K and of the maximum unramified extension $M_u \subset L$ and let $q = e_{L/M_t}$ be the ramification index for the maximum tamely ramified extension $M_t \subset L$.*

1. *The subgroup $G_0 \subset G$ equals the inertia subgroup $I \subset G$ corresponding to M_u. The action of G on the residue field E of L defines an isomorphism $G/G_0 \to \mathrm{Aut}(E/F)$.*

2. *The subgroup $G_1 \subset G$ equals the wild inertia subgroup $P \subset G$ corresponding to M_t. The character $I/P \to F'^\times$ (1.8) equals the q-th power of the character*

$$G_0 \to E^\times \tag{1.10}$$

defined by the action on an E-vector space $\mathfrak{m}_L/\mathfrak{m}_L^2$ of dimension 1.

Proof. 1. Since E is a purely inseparable extension of the separable closure $F' \subset E$ of F, the restriction defines an injection $\mathrm{Aut}(E/F) \to \mathrm{Gal}(F'/F)$. Hence we have $G_0 = I$ and the morphism $G/G_0 \to \mathrm{Aut}(E/F)$ is an isomorphism.

2. We have an exact sequence $0 \to E^\times \to L^\times/(1+\mathfrak{m}_L) \to \mathbf{Z} \to 0$ of G-modules. Since $G_0 = I = \mathrm{Ker}(G \to \mathrm{Aut}\, E) = \mathrm{Ker}(G \to \mathrm{Aut}\, E^\times)$ by 1, the exact sequence defines the character (1.10) and its kernel equals G_1.

To show the last assertion, we may assume that F is of characteristic $p > 0$ and that $q|[L : M_t]$ is a power of p by Corollary 1.5.6. By the canonical isomorphisms $\mathfrak{m}_{M_t}/\mathfrak{m}_{M_t}^2 \otimes_{F_s} E \to \mathfrak{m}_L^q/\mathfrak{m}_L^{q+1} \leftarrow (\mathfrak{m}_L/\mathfrak{m}_L^2)^{\otimes q}$, the character (1.8) equals the q-th power of the character (1.10). Since the character (1.10) is of order prime to p, the kernel G_1 of (1.10) equals the kernel P of the character (1.8). □

In the following, we assume that the residue field F is of characteristic $p > 0$. We study the graded quotients $\mathrm{Gr}_i G = G_i/G_{i+1}$ for $i \geqq 1$.

Proposition 1.6.3. *Assume that the residue field F is of characteristic $p > 0$. Let $i \geqq 1$ be an integer.*

1. *The action of G_i on $(1+\mathfrak{m}_L)/(1+\mathfrak{m}_L^{i+1})$ is trivial.*
2. *The action of G_i on $L^\times/(1+\mathfrak{m}_L^{i+1})$ defines a morphism*

$$\delta\colon G_i \to \mathrm{Hom}(L^\times/(1+\mathfrak{m}_L), \mathfrak{m}_L^i/\mathfrak{m}_L^{i+1}) \tag{1.11}$$

such that the kernel equals G_{i+1}. The image of $\sigma \in G_i$ is induced by the morphism $\delta_\sigma\colon L^\times \to \mathfrak{m}_L^i/\mathfrak{m}_L^{i+1}$ sending b to $\sigma(b)/b - 1 \bmod \mathfrak{m}_L^{i+1}$.

Proof. 1. For $\sigma \in G_i$ and $b \in \mathfrak{m}_L - \{0\}$, we have $\dfrac{\sigma(1+b)}{1+b} = 1 + \dfrac{\sigma(b)-b}{1+b} = 1 + \dfrac{b}{1+b}(\dfrac{\sigma(b)}{b} - 1) \in 1 + \mathfrak{m}_K^{i+1}$.

2. The subgroups $(1+\mathfrak{m}_L^i)/(1+\mathfrak{m}_L^{i+1}) \subset (1+\mathfrak{m}_L)/(1+\mathfrak{m}_L^{i+1})$ of $L^\times/(1+\mathfrak{m}_L^{i+1})$ are stable by the action of G and the actions of G_i on $L^\times/(1+\mathfrak{m}_L^i)$ and on $(1+\mathfrak{m}_L)/(1+\mathfrak{m}_L^{i+1})$ are trivial by 1. Hence, we obtain an injection $G_i/G_{i+1} \to \mathrm{Hom}(L^\times/(1+\mathfrak{m}_L), (1+\mathfrak{m}_L^i)/(1+\mathfrak{m}_L^{i+1}))$. By identifying $(1+\mathfrak{m}_L^i)/(1+\mathfrak{m}_L^{i+1})$ with $\mathfrak{m}_L^i/\mathfrak{m}_L^{i+1}$, we obtain (1.11). □

Corollary 1.6.4. *Let $i \geqq 1$ be an integer.*

1. *The morphism* (1.11) *induces an injection*

$$\mathrm{Gr}_i G \to \mathrm{Hom}(L^\times/(1+\mathfrak{m}_L), \mathfrak{m}_L^i/\mathfrak{m}_L^{i+1}) \tag{1.12}$$

compatible with the actions of G. The graded quotient $\mathrm{Gr}_i G = G_i/G_{i+1}$ is an $\mathbf{F}_p$-vector space.

2. *We have $[P, G_i] \subset G_{i+1}$. The injection* (1.12) *is compatible with the conjugate action of I/P on $\mathrm{Gr}_i G$ and the actions I/P on $L^\times/(1+\mathfrak{m}_L)$ and on the E-vector space $\mathfrak{m}_L^i/\mathfrak{m}_L^{i+1}$ by the i-th power of the character $I/P \to E^\times$* (1.10).

Proof. 1. Since the kernel of (1.11) is G_{i+1}, we obtain an injection (1.12). For $\sigma \in G_i$, $\tau \in G$ and $b \in L^\times$, we have

$$\delta_{\tau\sigma\tau^{-1}}\overline{b} \equiv \frac{\tau\sigma\tau^{-1}(b)}{b} - 1 = \tau\Big(\frac{\sigma(\tau^{-1}b)}{\tau^{-1}b} - 1\Big) = \tau(\delta_\sigma\overline{\tau^{-1}b}) = \tau(\delta_\sigma(\tau^{-1}\overline{b})).$$

Hence the injection (1.12) is compatible with the actions of G. Since $\mathfrak{m}_L^i/\mathfrak{m}_L^{i+1}$ is an E-vector space, the graded quotient $\mathrm{Gr}_i G$ is an $\mathbf{F}_p$-vector space.

2. Since the action of P on the target of the injection (1.12) is trivial, the conjugate action of P on G_i/G_{i+1} is trivial. This means $[P, G_i] \subset G_{i+1}$. The compatibility on the injection (1.12) follows from 1. □

We compare the two definitions of filtrations.

Proposition 1.6.5. *For an integer $i \geqq 1$, define $G_i' \subset G$ by $G_i' = \mathrm{Ker}(G \to \mathrm{Aut}(\mathcal{O}_L/\mathfrak{m}_L^i))$. Let $t \in L$ be a uniformizer.*

1. *Let $i \geqq 1$. Then, we have $G_i' = \mathrm{Ker}(G \to \mathrm{Aut}(\mathcal{O}_L/\mathfrak{m}_L^i)^\times)$ and*

$$G_{i+1}' \subset G_i = \{\sigma \in G_i' \mid \sigma(t)/t \equiv 1 \bmod \mathfrak{m}_L^i\} \subset G_i'. \tag{1.13}$$

2. *Assume that the residue field E is a separable extension of F. Then, for $i \geqq 1$, we have $G_i = G'_{i+1}$ and the morphism* (1.12) *induces an injection*

$$\delta\colon \mathrm{Gr}_i G \to \mathfrak{m}_L^i/\mathfrak{m}_L^{i+1}. \tag{1.14}$$

For $\sigma \in G_0$, we have

$$i(\sigma) = \mathrm{ord}_L(\sigma(t) - t) - 1.$$

3. *Assume $e_{L/K} = 1$. Then, for $i \geqq 1$, we have $G_i = G'_i$ and the morphism* (1.12) *induces an injection*

$$\delta\colon \mathrm{Gr}_i G \to \mathrm{Hom}(E^\times, \mathfrak{m}_L^i/\mathfrak{m}_L^{i+1}). \tag{1.15}$$

Further if $\mathcal{O}_L = \mathcal{O}_K[u]$, for $\sigma \in G_0$, we have

$$i(\sigma) = \mathrm{ord}_L(\sigma(u) - u).$$

Proof. 1. The inclusion $G'_i \subset \mathrm{Ker}(G \to \mathrm{Aut}(\mathcal{O}_L/\mathfrak{m}_L^i)^\times)$ is clear. Since the action of σ on $\mathcal{O}_L/\mathfrak{m}_L^i - (\mathcal{O}_L/\mathfrak{m}_L^i)^\times = \mathfrak{m}_L/\mathfrak{m}_L^i$ is trivial if and only if that on $(1+\mathfrak{m}_L)/(1+\mathfrak{m}_L^i) \subset (\mathcal{O}_L/\mathfrak{m}_L^i)^\times$ is trivial, we have the other inclusion.

We have $G_i \subset \mathrm{Ker}(G \to \mathrm{Aut}(\mathcal{O}_L/\mathfrak{m}_L^i)^\times) = G'_i$ since $(\mathcal{O}_L/\mathfrak{m}_L^i)^\times \subset L^\times/(1+\mathfrak{m}_L^i)$. By the exact sequence $0 \to (\mathcal{O}_L/\mathfrak{m}_L^i)^\times \to L^\times/(1+\mathfrak{m}_L^i) \to \mathbf{Z} \to 0$, we have the equality in (1.13). For $\sigma \in G'_{i+1}$, we have $\sigma(t) \equiv t \bmod \mathfrak{m}_L^{i+1}$. Hence the equality in (1.13) implies $G'_{i+1} \subset G_i$.

2. Since $G_0 = G'_1$, by replacing G by $I = G_0$, we may assume $G = I$. Then, we have $E = F$ and L is totally ramified over K. Since $\mathcal{O}_L = \mathcal{O}_K[t]$, we have $G'_{i+1} = \{\sigma \in G'_i \mid \sigma(t) \equiv t \bmod \mathfrak{m}_L^{i+1}\}$. This equals G_i by the equality in (1.13).

For $\sigma \in G_i = G'_{i+1}$, its image $\delta_\sigma\colon L^\times/(1+\mathfrak{m}_L) \to \mathfrak{m}_L^i/\mathfrak{m}_L^{i+1}$ by the injection (1.12) annihilates $E^\times \subset L^\times/(1+\mathfrak{m}_L)$ and defines an element $\mathrm{Hom}(\mathbf{Z}, \mathfrak{m}_L^i/\mathfrak{m}_L^{i+1}) = \mathfrak{m}_L^i/\mathfrak{m}_L^{i+1}$. Thus we obtain an injection (1.14).

Since $G_i = G'_{i+1} = \{\sigma \in G_0 \mid \sigma(t) - t \in \mathfrak{m}_K^{i+1}\}$, for $\sigma \in G_0$, the condition $\sigma \in G_i$ is equivalent to $\mathrm{ord}_L(\sigma(t) - t) \geqq i+1$.

3. Since $e_{L/K} = 1$, we may take $t \in \mathcal{O}_K$ and then the equality in (1.13) shows $G_i = G'_i$. For $\sigma \in G_i = G'_i$, its image $\delta_\sigma\colon L^\times/(1+\mathfrak{m}_L) \to \mathfrak{m}_L^i/\mathfrak{m}_L^{i+1}$ by the injection (1.12) annihilates the subgroup generated by a uniformizer $t \in K$ and defines an element $\mathrm{Hom}(E^\times, \mathfrak{m}_L^i/\mathfrak{m}_L^{i+1})$.

If $\mathcal{O}_L = \mathcal{O}_K[u]$, the condition $\sigma \in G'_i$ is equivalent to $\mathrm{ord}_L(\sigma(u) - u) \geqq i$. □

In the case where the ring of integers of the extension is generated by a single element, a relation with the filtration on quotient groups is given as follows.

Proposition 1.6.6. *Let L be a finite Galois extension of K of Galois group G. Let $N \subset G$ be a normal subgroup, $\overline{G} = G/N$ be the quotient group and let M be the corresponding extension. Let $F \subset F_M \subset E$ be the residue fields of $K \subset M \subset L$. Assume that either of the following conditions is satisfied:*

(1) *E is a separable extension of F_M.*

(2) *The ramification index $e_{L/M}$ is 1 and E is generated by a single element over F_M.*

Then, for $\sigma \in \overline{G}, \neq 1$, we have

$$e_{L/M} \cdot i_{\overline{G}}(\sigma) \leqq \sum_{\tau \in \sigma} i_G(\tau) \tag{1.16}$$

and the equality holds if either of the following conditions is satisfied:

(1_K) *E is a separable extension of F.*

(2_K) *The ramification index $e_{L/K}$ is 1 and E is generated by a single element over F.*

Proof. Since $\overline{G}_1 = \overline{P}$ is the image of $G_1 = P$, by replacing K by the maximum unramified extension $K' \subset L$, we may assume that either of the following conditions is satisfied:

($1'$) L is a totally ramified extension of M.

($2'$) The ramification index $e_{L/M}$ is 1 and E is a purely inseparable extension of F_M generated by a single element.

If L is a totally ramified extension of M, let t be a uniformizer of L. In the other case, let t be a generator of $\mathcal{O}_L$ over $\mathcal{O}_M$. Let $Q = X^m + b_1X^{m-1} + \cdots + b_m \in \mathcal{O}_M[X]$ be the minimal polynomial of t and set $s = b_m$ for $m = [L : M]$. Then, s is a uniformizer of M if L is totally ramified and s is a unit of $\mathcal{O}_M$ in the other case. Further in the case (2_K), s is a generator of $\mathcal{O}_M$ over $\mathcal{O}_K$. Hence, we have $i_{\overline{G}}(\sigma) \leqq \mathrm{ord}_M(\dfrac{\sigma(s)}{s} - 1)$ and the equality holds if (1_K) or (2_K) is satisfied.

Since $s = \pm \mathrm{N}_{L/M}t$, we have

$$\sum_{\tau \in \sigma} i_G(\tau) = \mathrm{ord}_L \frac{1}{s} \prod_{\tau \in \sigma} (t - \tau(t)). \tag{1.17}$$

Since $\sigma Q = X^m + \sigma(b_1)X^{m-1} + \cdots + \sigma(b_m) \in M[X]$ is the minimal polynomial of $\tau(t)$ for $\tau \in \sigma \subset G$, we have $\sigma Q = \prod_{\tau \in \sigma}(X - \tau(t))$ and $(\sigma Q)(t) = \prod_{\tau \in \sigma}(t - \tau(t))$. Since $Q(t) = 0$, we have $(\sigma Q)(t) = (\sigma Q - Q)(t) = \sum_{i=1}^{m}(\sigma(b_i) - b_i) \cdot t^{m-i}$. Hence we obtain

$$\frac{1}{s} \prod_{\tau \in \sigma} (t - \tau(t)) = \Big(\frac{\sigma(s)}{s} - 1\Big) + \sum_{i=1}^{m-1} \frac{b_i}{s} \Big(\frac{\sigma(b_i)}{b_i} - 1\Big) \cdot t^{m-i} \in \mathfrak{m}_L^{e_{L/M} \cdot i_{\overline{G}}(\sigma)}. \tag{1.18}$$

In the case ($1'$), Q is an Eisenstein polynomial and $b_i/s \in \mathcal{O}_M$ and $t^{m-i} \in \mathfrak{m}_L$ for $i = 1, \ldots, m-1$. In the case ($2'$), we have $b_i \in \mathfrak{m}_M$ for $i = 1, \ldots, m-1$. Hence we have (1.16) and a congruence

$$\frac{1}{s} \prod_{\tau \in \sigma} (t - \tau(t)) \equiv \frac{\sigma(s)}{s} - 1 \bmod \mathfrak{m}_L^{e_{L/M} \cdot i_{\overline{G}}(\sigma) + 1}. \tag{1.19}$$

Thus the equality $i_{\overline{G}}(\sigma) = \mathrm{ord}_M(\dfrac{\sigma(s)}{s} - 1)$ implies the equality in (1.16). □

Corollary 1.6.7. *Let L be a purely wildly ramified cyclic extension of degree p^2 and let M be the unique subextension. Let $G = \mathrm{Gal}(L/K)$ and $\overline{G} = \mathrm{Gal}(M/K)$ be the Galois groups and let $m_{L/K}$ and $m_{M/K}$ be the largest integers satisfying $G_m \neq 1$ or $\overline{G}_{m'} \neq 1$ respectively. Then, we have*

$$f_{L/M} \cdot m_{L/K} > m_{M/K}. \tag{1.20}$$

Proof. Let $l \leqq 1$ be the largest integer such that $G_l = G$. Then, since $\mathrm{Gr}_l G$ is annihilated by p by Corollary 1.6.4.1, we have $l < m_{L/K}$. Since $[L : M] = p$, one of (1) and (2) in Proposition 1.6.6 is satisfied and we have an inequality $e_{L/M} \cdot m_{M/K} \leqq p \cdot l$ by (1.16). Hence we obtain (1.20). □

Exercise 1.6. Let p be a prime number and $n \geqq 1$ be an integer. Identify the Galois group $G = \mathrm{Gal}(\mathbf{Q}_p(\zeta_{p^n})/\mathbf{Q}_p)$ with $(\mathbf{Z}/p^n\mathbf{Z})^\times$. Compute the lower numbering filtration G_i.

Solution. For $1 < a < p^n$ prime to p, let $\sigma_a \in G$ be the element corresponding to $a \in (\mathbf{Z}/p^n\mathbf{Z})^\times$. Then, for $0 \leqq m = \mathrm{ord}_p(a-1) < n$, we have $i_G(\sigma_a) = \mathrm{ord}(\zeta_{p^n}^a - \zeta_{p^n}) = \mathrm{ord}(\zeta_{p^n}^{a-1} - 1) = \mathrm{ord}(\zeta_{p^n}^{p^m} - 1) = p^m$. Hence $G_i = 1 + (p^m) \subset (\mathbf{Z}/p^n\mathbf{Z})^\times = \mathrm{Gal}(\mathbf{Q}_p(\zeta_{p^n})/\mathbf{Q}_p)$ for $p^{m-1} \leqq i < p^m$ for $1 \leqq m < n$, $G_i = 1$ for $i \geqq p^{n-1}$ and $G = G_0$.

1.7 Different

We study the morphism $\mathrm{Tr}_{L/K}$ for finite extensions L of a henselian discrete valuation field K.

Proposition 1.7.1. *Let L be a finite separable extension of a henselian discrete valuation field K.*

1. *We have $\mathrm{Tr}_{L/K}(\mathcal{O}_L) \subset \mathcal{O}_K$, $\mathrm{Tr}_{L/K}(\mathfrak{m}_L) \subset \mathfrak{m}_K$ and the diagram*

$$\begin{array}{ccc} \mathcal{O}_L & \longrightarrow & E \\ {\scriptstyle \mathrm{Tr}_{L/K}}\big\downarrow & & \big\downarrow{\scriptstyle e_{L/K}\cdot \mathrm{Tr}_{E/F}} \\ \mathcal{O}_K & \longrightarrow & F \end{array} \tag{1.21}$$

is commutative. The $\mathcal{O}_L$-modules $\mathrm{Hom}_{\mathcal{O}_K}(\mathfrak{m}_L, \mathfrak{m}_K) = \mathfrak{m}_L^{-1}\mathfrak{m}_K \cdot \mathrm{Hom}_{\mathcal{O}_K}(\mathcal{O}_L, \mathcal{O}_K) \subset \mathrm{Hom}_{\mathcal{O}_K}(\mathcal{O}_L, \mathcal{O}_K)$ are free of rank 1.

2. *The following conditions are equivalent:*
(1) *L is tamely ramified over K.*
(2) *$\mathrm{Tr}_{L/K}$ is a basis of the free $\mathcal{O}_L$-module $\mathrm{Hom}_{\mathcal{O}_K}(\mathfrak{m}_L, \mathfrak{m}_K)$.*
(3) *The morphism $\mathrm{Tr}_{L/K} \colon \mathcal{O}_L \to \mathcal{O}_K$ is a surjection.*

3. *The following conditions are equivalent:*
(1) *L is unramified over K.*
(2) *$\mathrm{Tr}_{L/K}$ is a basis of the free $\mathcal{O}_L$-module $\mathrm{Hom}_{\mathcal{O}_K}(\mathcal{O}_L, \mathcal{O}_K)$.*

Proof. 1. Since $\mathrm{Tr}_{L/K}$ is the base change of $\mathrm{Tr}_{\mathcal{O}_L/\mathcal{O}_K} \colon \mathcal{O}_L \to \mathcal{O}_K$, we have $\mathrm{Tr}_{L/K}(\mathcal{O}_L) \subset \mathcal{O}_K$. Since $\mathcal{O}_L/\mathfrak{m}_K\mathcal{O}_L$ is a successive extension of $\mathfrak{m}_L^i/\mathfrak{m}_L^{i+1}$ for $i = 0, \ldots, e-1$, the diagram (1.21) is commutative. The inclusion $\mathrm{Tr}_{L/K}(\mathfrak{m}_L) \subset \mathfrak{m}_K$ follows from the commutative diagram (1.21).

Since $\mathrm{Hom}_{\mathcal{O}_K}(\mathcal{O}_L, \mathcal{O}_K)$ is a free $\mathcal{O}_K$-module of rank $[L : K]$, it is a free $\mathcal{O}_L$-module of rank 1. Hence $\mathrm{Hom}_{\mathcal{O}_K}(\mathfrak{m}_L, \mathfrak{m}_K) = \mathfrak{m}_L^{-1}\mathfrak{m}_K \cdot \mathrm{Hom}_{\mathcal{O}_K}(\mathcal{O}_L, \mathcal{O}_K)$ is also a free $\mathcal{O}_L$-module of rank 1.

2. (1)$\Leftrightarrow$(3): By the commutative diagram (1.21) and by Nakayama's lemma, the surjectivity of $\mathrm{Tr}_{L/K} \colon \mathcal{O}_L \to \mathcal{O}_K$ is equivalent to the surjectivity of $e_{L/K} \cdot \mathrm{Tr}_{E/F} \colon E \to F$. The latter condition is equivalent to that E is a separable extension of F and that $e_{L/K}$ is invertible in F.

(2)$\Leftrightarrow$(3): Since $\mathrm{Hom}_{\mathcal{O}_K}(\mathfrak{m}_L, \mathfrak{m}_K) = \mathfrak{m}_L^{-1}\mathrm{Hom}_{\mathcal{O}_K}(\mathcal{O}_L, \mathfrak{m}_K)$, we obtain an exact sequence $0 \to \mathrm{Hom}_{\mathcal{O}_K}(\mathcal{O}_L, \mathfrak{m}_K) \to \mathrm{Hom}_{\mathcal{O}_K}(\mathfrak{m}_L, \mathfrak{m}_K) \to \mathrm{Hom}_F(E, F) \to 0$ where the second arrow maps $f \in \mathrm{Hom}_{\mathcal{O}_K}(\mathfrak{m}_L, \mathfrak{m}_K) \subset \mathrm{Hom}_{\mathcal{O}_K}(\mathcal{O}_L, \mathcal{O}_K)$ to the induced morphism $\overline{f} \colon E \to F$. Hence the equivalence follows from Nakayama's lemma.

3. Since $\mathrm{Hom}_{\mathcal{O}_K}(\mathfrak{m}_L, \mathfrak{m}_K) = \mathfrak{m}_L^{-1}\mathfrak{m}_K \cdot \mathrm{Hom}_{\mathcal{O}_K}(\mathcal{O}_L, \mathcal{O}_K) \subset \mathrm{Hom}_{\mathcal{O}_K}(\mathcal{O}_L, \mathcal{O}_K)$ and the equality holds if and only if $e_{L/K} = 1$, the assertion follows from 2 (1)$\Leftrightarrow$(2). □

We define the different and its logarithmic variant for a finite separable extension of discrete valuation fields.

Definition 1.7.2. *Let L be a finite separable extension of a henselian discrete valuation field K. Define the different and the logarithmic different $D_{L/K} \subset D_{L/K}^{\log} \subset \mathcal{O}_L$ to be the ideals satisfying*

$$\mathcal{O}_L \cdot \mathrm{Tr}_{L/K} = D_{L/K} \cdot \mathrm{Hom}_{\mathcal{O}_K}(\mathcal{O}_L, \mathcal{O}_K) = D_{L/K}^{\log} \cdot \mathrm{Hom}_{\mathcal{O}_K}(\mathfrak{m}_L, \mathfrak{m}_K).$$

Since $\mathrm{Hom}_{\mathcal{O}_K}(\mathfrak{m}_L, \mathfrak{m}_K) = \mathfrak{m}_L^{-1}\mathfrak{m}_K \cdot \mathrm{Hom}_{\mathcal{O}_K}(\mathcal{O}_L, \mathcal{O}_K)$, we have $D_{L/K} = \mathfrak{m}_L^{-1}\mathfrak{m}_K \cdot D_{L/K}^{\log}$.

Lemma 1.7.3. *Let L be a finite separable extension of a henselian discrete valuation field K.*

1. *We have $\mathrm{Tr}_{L/K} D_{L/K}^{\log\,-1} = \mathcal{O}_K$ and $\mathrm{Tr}_{L/K}(\mathfrak{m}_L D_{L/K}^{\log\,-1}) = \mathfrak{m}_K$. There exists a generator b of $D_{L/K}^{\log\,-1}$ satisfying $\mathrm{Tr}_{L/K} b = 1$.*
2. *Let $M \subset L$ be a subextension over K. Then, we have*

$$D_{L/K} = D_{M/K} \cdot D_{L/M}, \tag{1.22}$$

$$D_{L/K}^{\log} = D_{M/K}^{\log} \cdot D_{L/M}^{\log}. \tag{1.23}$$

The equalities (1.22) and (1.23) are called the chain rules.

Proof. 1. Since $\mathrm{Tr}_{L/K}$ is a generator of $D_{L/K}^{\log} \cdot \mathrm{Hom}_{\mathcal{O}_K}(\mathfrak{m}_L, \mathfrak{m}_K)$, we have $\mathrm{Tr}_{L/K}(\mathfrak{m}_L D_{L/K}^{\log\,-1}) \subset \mathfrak{m}_K$ and $\mathrm{Tr}_{L/K}(D_{L/K}^{\log\,-1}) \not\subset \mathfrak{m}_K$. Since $\mathrm{Tr}_{L/K}(\mathfrak{m}_K D_{L/K}^{\log\,-1}) \subset \mathrm{Tr}_{L/K}(\mathfrak{m}_L D_{L/K}^{\log\,-1})$, the first inclusion implies $\mathrm{Tr}_{L/K}(D_{L/K}^{\log\,-1}) \subset \mathcal{O}_K$. Hence we obtain the equalities.

By $\mathrm{Tr}_{L/K}(D_{L/K}^{\log\,-1}) = \mathcal{O}_K$, there exists an element $b \in D_{L/K}^{\log\,-1}$ satisfying $\mathrm{Tr}_{L/K} b = 1$. Since $\mathrm{Tr}_{L/K}(\mathfrak{m}_L D_{L/K}^{\log\,-1}) = \mathfrak{m}_K$, the element b is not contained in $\mathfrak{m}_L D_{L/K}^{\log\,-1}$ and is a generator of $D_{L/K}^{\log\,-1}$

2. The equality (1.22) follows from the canonical isomorphism $\mathrm{Hom}_{\mathcal{O}_K}(\mathcal{O}_M, \mathcal{O}_K) \otimes_{\mathcal{O}_M} \mathrm{Hom}_{\mathcal{O}_M}(\mathcal{O}_L, \mathcal{O}_M) \to \mathrm{Hom}_{\mathcal{O}_K}(\mathcal{O}_L, \mathcal{O}_K)$ and $\mathrm{Tr}_{M/K} \circ \mathrm{Tr}_{L/M} = \mathrm{Tr}_{L/K}$. The second equality (1.23) follows from the first equality (1.22). □

We state a criterion in terms of the different for the extension to be unramified or tamely ramified.

Lemma 1.7.4. *Let L be a finite separable extension of a henselian discrete valuation field K.*

1. *The following conditions are equivalent:*
(1) *L is tamely ramified over K.*
(2) *We have $D_{L/K}^{\log} = \mathcal{O}_L$.*
2. *The following conditions are equivalent:*
(1) *L is unramified over K.*
(2) *We have $D_{L/K} = \mathcal{O}_L$.*

Proof. They follow from Proposition 1.7.1.2 and 3 respectively. □

We compute the different assuming that the ring of integers is generated by a single element over $\mathcal{O}_K$.

Proposition 1.7.5. *Let K be a henselian discrete valuation field and let L be a finite separable extension of degree n of K.*

1. *Assume that $\mathcal{O}_L$ is generated by $b \in \mathcal{O}_L$ over $\mathcal{O}_K$ and let $P \in \mathcal{O}_K[X]$ be the minimal polynomial of b. Then, the different $D_{L/K}$ is generated by $P'(b)$.*

2. *Assume that L is a Galois extension of Galois group G. Assume that either of the following conditions is satisfied:*
(1) *E is a separable extension of F.*
(2) *The ramification index $e_{L/K}$ is 1 and E is generated by a single element over F.*

Then, we have

$$\mathrm{ord}_L D^{\log}_{L/K} = \sum_{\sigma\in G,\,\sigma\neq 1} i_G(\sigma). \tag{1.24}$$

The relation between the different and the lower ramification groups proved in Proposition 1.7.5.2 is called the conductor–discriminant formula.

Proof. 1. By Proposition 1.2.2, we have $\mathcal{O}_L \cdot \mathrm{Tr}_{L/K} = P'(b) \cdot \mathrm{Hom}_{\mathcal{O}_K}(\mathcal{O}_L, \mathcal{O}_K)$.

2. By replacing K by the maximum unramified extension $M \subset L$, we may assume that either of the following conditions is satisfied:

($1'$) L is a totally ramified extension of K.

($2'$) The ramification index $e_{L/K}$ is 1 and E is a purely inseparable extension of F generated by a single element.

If L is a totally ramified extension of K, let t be a uniformizer. In the other case, let t be a generator of $\mathcal{O}_L$ over $\mathcal{O}_K$. By Proposition 1.6.3.2, we have $i_G(\sigma) = \mathrm{ord}_L(\sigma(t) - t)/t$. Let $P \in \mathcal{O}_K[T]$ be the minimal polynomial of t. Then, by 1, we have $\mathrm{ord}_L D^{\log}_{L/K} = \mathrm{ord}_L P'(t)/t^{n-1}$ for $n = [L : K]$. Hence, the equality follows from $P'(t) = \prod_{\sigma\in G}(t - \sigma(t))$. □

Corollary 1.7.6. *Let $N \subset G = \mathrm{Gal}(L/K)$ be a normal subgroup and identify the Galois group $\overline{G} = \mathrm{Gal}(L/M)$ of the corresponding extension $M \subset L$ with the quotient group G/N. Then, we have*

$$e_{L/M} \cdot \mathrm{ord}_M D^{\log}_{M/K} = \mathrm{ord}_L D^{\log}_{L/K} - \sum_{\tau\in N - \{1\}} i_G(\tau).$$

Proof. By the chain rule Lemma 1.7.3.2, we have $e_{L/M}\cdot\mathrm{ord}_M D^{\log}_{M/K} + \mathrm{ord}_L D^{\log}_{L/M} = \mathrm{ord}_L D^{\log}_{L/K}$. Thus the equality follows from Proposition 1.7.5.2. □

Exercise 1.7. Let p be a prime number and $n \geqq 1$ be an integer.

1. Find a generator of the different $D_{\mathbf{Q}_p(\zeta_{p^n})/\mathbf{Q}_p}$.

2. Find a generator b of the inverse $(D^{\log}_{\mathbf{Q}_p(\zeta_{p^n})/\mathbf{Q}_p})^{-1}$ of the logarithmic different such that $\mathrm{Tr}_{\mathbf{Q}_p(\zeta_{p^n})/\mathbf{Q}_p} b = 1$.

Solution. 1. The cyclotomic polynomial Φ_{p^n} is the minimal polynomial of ζ_{p^n}. Since $\Phi'_p = ((X^p - 1)/(X - 1))' = (pX^{p-1}(X - 1) - (X^p - 1))/(X - 1)^2$, we have $\Phi'_p(\zeta_p) = p/(\zeta_p(\zeta_p - 1))$. Since $\Phi_{p^n} = \Phi_p(X^{p^{n-1}})$, we have $\Phi'_{p^n} = \Phi'_p(X^{p^{n-1}}) \cdot p^{n-1}X^{p^{n-1}-1}$ and $\Phi'_{p^n}(\zeta_{p^n}) = \Phi'_p(\zeta_p) \cdot p^{n-1}\zeta_p/\zeta_{p^n} = p^n/(\zeta_{p^n}(\zeta_p - 1))$. Hence by Proposition 1.7.5.1, the different $D_{\mathbf{Q}_p(\zeta_{p^n})/\mathbf{Q}_p}$ is generated by $p^n/(\zeta_p - 1)$.

2. By the solution of 1, $b = -\zeta_{p^n}(\zeta_p - 1)/p^n \cdot p/(\zeta_{p^n} - 1) = -\sum_{i=1}^{p^{n-1}} \zeta^i_{p^n}/p^{n-1}$ is a generator of $(D^{\log}_{\mathbf{Q}_p(\zeta_{p^n})/\mathbf{Q}_p})^{-1}$. Since $\mathrm{Tr}_{\mathbf{Q}_p(\zeta_{p^n})/\mathbf{Q}_p(\zeta_p)}\zeta^i_{p^n} = 0$ for $i = 1, \ldots, p^{n-1} - 1$, we have $\mathrm{Tr}_{\mathbf{Q}_p(\zeta_{p^n})/\mathbf{Q}_p} b = -p^{n-1}\mathrm{Tr}_{\mathbf{Q}_p(\zeta_p)/\mathbf{Q}_p}\zeta_p/p^{n-1} = 1$.

1.8 Norm

Let L be a finite extension of a henselian discrete valuation field K and let $\mathrm{N}_{L/K} \colon L^\times \to K^\times$ be the norm mapping. We consider the filtration of $L^\times$ defined by $1 + \mathfrak{m}^i_L$ for integers $i \geqq 1$ and study the images $\mathrm{N}_{L/K}(1 + \mathfrak{m}^i_L) \subset K^\times$.

Lemma 1.8.1. *Let L be a finite extension of K.*

1. *Let $n = [L : K]$ and $e_{L/K}$ be the ramification index. Then, the diagram*

$$\begin{array}{ccc} L^\times & \xrightarrow{\mathrm{ord}_L} & \mathbf{Z} \\ {\scriptstyle \mathrm{N}_{L/K}}\downarrow & & \downarrow{\scriptstyle \times n/e_{L/K}} \\ K^\times & \xrightarrow{\mathrm{ord}_K} & \mathbf{Z} \end{array} \tag{1.25}$$

is commutative.

2. *For any integer $i \geqq 0$, we have*

$$\mathrm{N}_{L/K}(1 + \mathfrak{m}_K^{i+1}\mathcal{O}_L) \subset \mathrm{N}_{L/K}(1 + \mathfrak{m}_K^i \mathfrak{m}_L) \subset 1 + \mathfrak{m}_K^{i+1}.$$

For $i \geqq 1$ and $x \in \mathfrak{m}_K^i \mathcal{O}_L$, we have

$$\mathrm{N}_{L/K}(1 + x) \equiv 1 + \mathrm{Tr}_{L/K} x \mod \mathfrak{m}_K^{i+1}. \tag{1.26}$$

Proof. 1. Since $\mathrm{N}_{L/K}\mathcal{O}_L^\times \subset \mathcal{O}_K^\times$, there exists a unique integer f such that the multiplication by f on the right vertical arrow makes the diagram (1.25) commutative. Since $\mathrm{ord}_K \mathrm{N}_{L/K} t = n$ and $\mathrm{ord}_L t = e_{L/K}$ for a uniformizer $t \in K^\times$, we have $f = n/e_{L/K}$.

2. Let $b \in L$ and $\mathrm{N}_{L/K}(X + b) = X^n + a_1 X^{n-1} + \cdots + a_n \in K[X]$ be the characteristic polynomial of $-b$. Then, we have $a_1 = \mathrm{Tr}_{L/K} b$, $a_n = \mathrm{N}_{L/K} b$ and

$$\mathrm{N}_{L/K}(1 + xb) = 1 + a_1 x + a_2 x^2 + \cdots + a_n x^n \tag{1.27}$$

for $x \in K$. If $b \in \mathfrak{m}_L$, the multiplication by b on the F-vector space $\mathcal{O}_L/\mathfrak{m}_K\mathcal{O}_L$ is nilpotent and we have $a_1, \ldots, a_n \in \mathfrak{m}_K$. Thus, we have the second inclusion by (1.27). The first inclusion follows from $\mathfrak{m}_K \mathcal{O}_L \subset \mathfrak{m}_L$

If $b \in \mathcal{O}_L$, we have $a_1, \ldots, a_n \in \mathcal{O}_K$. Hence the congruence (1.26) follows from (1.27) for $x \in \mathfrak{m}_K^i$ and $a_1 = \mathrm{Tr}_{L/K} b$. □

We show an inclusion in the opposite direction.

Lemma 1.8.2. *Let L be a finite separable extension of K of degree n. Let $c \in \mathfrak{m}_L$ be an non-zero element, $j = \mathrm{ord}_L c$ and and let $\mathrm{N}_{L/K}(X + c) = X^n + a_1 X^{n-1} + \cdots + a_n$ be the characteristic polynomial of $-c$. Assume $\mathrm{Tr}_{L/K} c = a_1 \neq 0$ and let $i = \mathrm{ord}_K a_1 \geqq 1$. Assume further that $\mathrm{ord}_K a_q > i$ for every $q = 2, \ldots, n = [L : K]$. Then, we have*

$$1 + \mathfrak{m}_K^i \subset \mathrm{N}_{L/K}(1 + \mathfrak{m}_L^j). \tag{1.28}$$

Proof. The polynomial

$$P = \frac{1}{a_1} \cdot (\mathrm{N}_{L/K}(1 + cX) - 1) = X + \sum_{q=2}^{n} \frac{a_q}{a_1} X^q$$

has coefficients in $\mathfrak{m}_K$ except for degree 1 by the assumption $\mathrm{ord}_K a_q > i$ for every $q = 2, \ldots, n$. Let $z = a_1 w$ be any element of $\mathfrak{m}_K^i$. Since $\mathcal{O}_K$ is henselian and $P(w) \equiv w$, $P'(w) \equiv 1 \bmod \mathfrak{m}_K$, there exists $x \in \mathcal{O}_K$ such that $P(x) = w$ by Hensel's lemma. Since $\mathrm{N}_{L/K}(1 + cx) = 1 + a_1 P(x) = 1 + z$, we obtain the inclusion (1.28). □

We have a characterization of tamely ramified extensions.

Proposition 1.8.3. *Let L be a finite separable extension of a henselian discrete valuation field K.*

1. *Let $d_{L/K}$ be the valuation of logarithmic different $D^{\log}_{L/K}$, $e_{L/K}$ the ramification index and let $i \geqq 1$ be an integer satisfying $e_{L/K} \cdot i > d_{L/K}$. Then, we have*

$$1 + \mathfrak{m}_K^{2i} \subset \mathrm{N}_{L/K}(1 + \mathfrak{m}_K^i \mathfrak{m}_L) \subset \mathrm{N}_{L/K}(1 + \mathfrak{m}_L). \tag{1.29}$$

2. *The following conditions are equivalent:*
(1) *L is a tamely ramified extension of K.*
(2) *We have $\mathrm{N}_{L/K}(1 + \mathfrak{m}_K^i \mathcal{O}_L) = 1 + \mathfrak{m}_K^i$ for every $i \geqq 1$.*
(3) *We have $\mathrm{N}_{L/K}(1 + \mathfrak{m}_K \mathcal{O}_L) = 1 + \mathfrak{m}_K$.*

If these equivalent conditions hold, we have $\mathrm{N}_{L/K}(1 + \mathfrak{m}_K^i \mathfrak{m}_L) = 1 + \mathfrak{m}_K^{i+1}$ for every $i \geqq 0$.

Proof. 1. Let $a \in \mathfrak{m}_K^i$ be an element with valuation $\mathrm{ord}_K a = i$ and let $b \in (D^{\log}_{L/K})^{-1}$ be a generator satisfying $\mathrm{Tr}_{L/K} b = 1$ as in Lemma 1.7.3.1. Let $\mathrm{N}_{L/K}(X + b) = X^n + X^{n-1} + a_2 X^{n-2} + \cdots + a_n$ be the characteristic polynomial of $-b$. Then, by $e_{L/K} \cdot i > d_{L/K}$, we have $ab \in \mathfrak{m}_L$ and hence $a^q a_q \in \mathfrak{m}_K$ for $q \geqq 2$. For $c = a^2 b \in \mathfrak{m}_K^i \mathfrak{m}_L$, the coefficients of $\mathrm{N}_{L/K}(X + c) = X^n + a^2 X^{n-1} + a^4 a_2 X^{n-2} + \cdots + a^{2n} a_n$ satisfy $2i = \mathrm{ord}_K a^2 < \mathrm{ord}_K a^{2q} a_q$ for $q = 2, \ldots, n$. Hence we have (1.29) by Lemma 1.8.2.

2. (1)⇒(2): Assume that L is a tamely ramified extension and $i \geqq 1$. By Lemma 1.8.1.2, we have $\mathrm{N}_{L/K}(1 + \mathfrak{m}_K^i \mathcal{O}_L) \subset 1 + \mathfrak{m}_K^i$. Since $D^{\log}_{L/K} = \mathcal{O}_L$ by Lemma 1.7.4.1 (1)⇒(2), there exists a unit $b \in \mathcal{O}_L^\times$ satisfying $\mathrm{Tr}_{L/K} b = 1$ by Lemma 1.7.3.1. Let $a \in \mathfrak{m}_K^i$ be a generator. Then, for a generator $c = ab$ of $\mathfrak{m}_K^i \mathcal{O}_L$, we have $\mathrm{Tr}_{L/K} c = a \mathrm{Tr}_{L/K} b = a$ and $\mathrm{N}_{L/K}(X + c) \equiv X^n + aX^{n-1} \bmod \mathfrak{m}_K^{2i}$. Hence we have the other inclusion by Lemma 1.8.2.

(2)⇒(3) is trivial.

(3)⇒(1): Assume $\mathrm{N}_{L/K}(1 + \mathfrak{m}_K \mathcal{O}_L) = 1 + \mathfrak{m}_K$. For $x \in \mathfrak{m}_K \mathcal{O}_L$, we have $\mathrm{N}_{L/K}(1 + x) \equiv 1 + \mathrm{Tr}_{L/K} x \bmod \mathfrak{m}_K^2$ by (1.26). Hence, $\mathrm{Tr}_{L/K}$ induces a surjection $\mathfrak{m}_K \mathcal{O}_L \to \mathfrak{m}_K / \mathfrak{m}_K^2$. By Nakayama's lemma, $\mathrm{Tr}_{L/K} \colon \mathfrak{m}_K \mathcal{O}_L \to \mathfrak{m}_K$ is a surjection. Hence the assertion follows from Proposition 1.7.1.2 (3)⇒(1).

The equality $\mathrm{N}_{L/K}(1 + \mathfrak{m}_K^{i+1} \mathcal{O}_L) = 1 + \mathfrak{m}_K^{i+1}$ implies $\mathrm{N}_{L/K}(1 + \mathfrak{m}_K^i \mathfrak{m}_L) = 1 + \mathfrak{m}_K^{i+1}$ by Lemma 1.8.1.2. □

We compute the norm mapping for cyclic extension of degree p. This will be used both in the first case and in the induction step of the proof of Theorem 4.4.4.

Lemma 1.8.4. *Let L be a cyclic extension of degree p of K of Galois group G. Let $d_{L/K}$ be the valuation of logarithmic different $D^{\log}_{L/K}$, $e_{L/K}$ the ramification index and $f_{L/K} = [E : F]$. For $x \in L$, let $X^p + a_1(x) X^{p-1} + \cdots + a_p(x) \in K[X]$ be the characteristic polynomial of $-x$ and $\mathrm{Tr}_{L/K} x = a_1(x)$, $\mathrm{N}_{L/K} x = a_p(x)$. Let i and j be integers satisfying $j - 1 \geqq e_{L/K} \cdot (i - 1) - d_{L/K}$.*

1. *For any $x \in \mathfrak{m}_L^j$, we have*

$$\mathrm{Tr}_{L/K} x \in \mathfrak{m}_K^i, \quad \mathrm{N}_{L/K} x \in \mathfrak{m}_K^{f_{L/K} \cdot j}, \quad a_q(x) \in \mathfrak{m}_K^i \text{ for } 2 \leqq q \leqq p - 1. \tag{1.30}$$

2. *Further if $2j - 1 \geqq e_{L/K} \cdot i - d_{L/K}$, we may replace $\mathfrak{m}_K^i$ by $\mathfrak{m}_K^{i+1}$ for $2 \leqq q \leqq p - 1$.*

Proof. 1. Since $\mathrm{Tr}_{L/K}(\mathfrak{m}_L^{-(d_{L/K} + e_{L/K} - 1)}) = \mathrm{Tr}_{L/K}(D^{\log}_{L/K}) \subset \mathcal{O}_K$ by Lemma 1.7.3.1, the inequality $j + d_{L/K} + e_{L/K} - 1 \geqq e_{L/K} \cdot i$ implies $\mathrm{Tr}_{L/K}(\mathfrak{m}_L^j) \subset \mathfrak{m}_K^i$.

By Lemma 1.8.1.1, the condition $x \in \mathfrak{m}_L^j$ implies $\mathrm{N}_{L/K}x \in \mathfrak{m}_K^{[E:F]\cdot j}$.

Let $2 \leqq q \leqq p-1$. Let S_q denote the set of subsets of $G = \mathrm{Gal}(L/K)$ with q elements. Then, we have $a_q(x) = \sum_{A \in S_q} \prod_{\sigma \in A} \sigma(x)$. The group G acts on S_q without fixed point. Let $T_q \subset S_q$ be a complete set of representatives with respect to the action of G. Then, the right hand side equals $\sum_{A \in T_q} \mathrm{Tr}_{L/K}(\prod_{\sigma \in A} \sigma(x))$. Since $\prod_{\sigma \in A} \sigma(x) \in \mathfrak{m}_L^{2j} \subset \mathfrak{m}_L^j$, we have $\mathrm{Tr}_{L/K}(\prod_{\sigma \in A} \sigma(x)) \in \mathfrak{m}_K^i$.

2. If $2j + d_{L/K} + e_{L/K} - 1 \geqq e_{L/K} \cdot (i+1)$, further we have $\mathrm{Tr}_{L/K}(\prod_{\sigma \in A} \sigma(x)) \in \mathrm{Tr}_{L/K}(\mathfrak{m}_L^{2j}) \subset \mathfrak{m}_K^{i+1}$. □

Proposition 1.8.5. *Let K be a henselian discrete valuation field and let L be a wildly ramified cyclic extension of K of degree p of Galois group G. Let $d_{L/K}$, $e_{L/K}$ denote the valuation of the logarithmic different and the ramification index and let $m_{L/K} \geqq 1$ denote the largest integer such that $G_m \neq 1$.*

1. *Let $j > m_{L/K}$ be an integer such that $e_{L/K} \mid j + d_{L/K} = e_{L/K} \cdot i$. Then, we have*

$$\begin{aligned} \mathrm{N}_{L/K}(1+\mathfrak{m}_L^j) &= 1+\mathfrak{m}_K^i, \qquad \mathrm{N}_{L/K}(1+\mathfrak{m}_L^{j+1}) = 1+\mathfrak{m}_K^{i+1}, \\ \mathrm{Tr}_{L/K}(1+\mathfrak{m}_L^j) &= 1+\mathfrak{m}_K^i, \qquad \mathrm{Tr}_{L/K}(1+\mathfrak{m}_L^{j+1}) = 1+\mathfrak{m}_K^{i+1} \end{aligned} \tag{1.31}$$

and the diagram

$$\begin{array}{ccc} \mathfrak{m}_L^j/\mathfrak{m}_L^{j+1} & \longrightarrow & 1+\mathfrak{m}_L^j/1+\mathfrak{m}_L^{j+1} \\ {\scriptstyle \mathrm{Tr}_{L/K}}\downarrow & & \downarrow{\scriptstyle \mathrm{N}_{L/K}} \\ \mathfrak{m}_K^i/\mathfrak{m}_K^{i+1} & \longrightarrow & 1+\mathfrak{m}_K^i/1+\mathfrak{m}_K^{i+1} \end{array} \tag{1.32}$$

is commutative.

2. *Let $1 \leqq j \leqq m_{L/K}$ be an integer and set $1 \leqq i = f_{L/K} \cdot j \leqq f_{L/K} \cdot m_{L/K}$. Then, we have $\mathrm{N}_{L/K}(1+\mathfrak{m}_L^j) \subset 1+\mathfrak{m}_K^i$, $\mathrm{N}_{L/K}(1+\mathfrak{m}_L^{j+1}) \subset 1+\mathfrak{m}_K^{i+1}$ and the diagram*

$$\begin{array}{ccc} \mathfrak{m}_L^j/\mathfrak{m}_L^{j+1} & \longrightarrow & (1+\mathfrak{m}_L^j)/(1+\mathfrak{m}_L^{j+1}) \\ \downarrow & & \downarrow{\scriptstyle \mathrm{N}_{L/K}} \\ \mathfrak{m}_K^i/\mathfrak{m}_K^{i+1} & \longrightarrow & (1+\mathfrak{m}_K^i)/(1+\mathfrak{m}_K^{i+1}) \end{array} \tag{1.33}$$

where the left vertical arrow is $\mathrm{Tr}_{L/K} + \mathrm{N}_{L/K}$ if $j = m_{L/K}$ and is $\mathrm{N}_{L/K}$ if $1 \leqq j < m_{L/K}$ is commutative.

Proof. 1. Let $j > m_{L/K}$ be an integer not necessarily satisfying $e_{L/K} \mid j + d_{L/K}$ and let $i > f_{L/K} \cdot m_{L/K}$ be the smallest integer satisfying $j \leqq e_{L/K} \cdot i - d_{L/K}$. In the notation of Lemma 1.8.4, for $x \in \mathfrak{m}_L^j$, we have

$$\mathrm{N}_{L/K}(1+x) = 1 + a_1(x) + a_2(x) + \cdots + a_p(x). \tag{1.34}$$

We have $a_q(x) \in \mathfrak{m}_K^i$ for $q = 1, \ldots, p$ by $j - 1 \geqq e_{L/K} \cdot (i-1) - d_{L/K}$, $f_{L/K} \cdot j \geqq i$ and Lemma 1.8.4.1. Hence by (1.34), we have an inclusion $\mathrm{N}_{L/K}(1+\mathfrak{m}_L^j) \subset 1+\mathfrak{m}_K^i$ in (1.31).

We show the other inclusion assuming $e_{L/K} \mid j + d_{L/K} = e_{L/K} \cdot i$. Let $b \in D_{L/K}^{\log -1}$ be a generator such that $\mathrm{Tr}_{L/K} b = 1$ as in Lemma 1.7.3.1. The integer $j = e_{L/K} \cdot i - (p-1) \cdot m_{L/K} \geqq e_{L/K} + m_{L/K}$ satisfies $2j - 1 \geqq e_{L/K} \cdot i - (p-1) \cdot m_{L/K} + e_{L/K} +$

$m_{L/K} - 1 \geqq e_{L/K} \cdot (i+1) - (p-1) \cdot m_{L/K}$. Hence for $a \in \mathfrak{m}_K^i$, $c = ab \in \mathfrak{m}_L^j$ and for $q = 2, \ldots, p-1$, we have $a_q(c) \in \mathfrak{m}_K^{i+1}$ by Lemma 1.8.4.1. For $q = p$, we have $\mathrm{ord}_K a_p(c) = \mathrm{ord}_K \mathrm{N}_{L/K} c \geqq f_{L/K} \cdot j > i$ since $j > m_{L/K}$. Thus by Lemma 1.8.2, we obtain the other inclusion $\mathrm{N}_{L/K}(1+\mathfrak{m}_L^j) \supset 1+\mathfrak{m}_K^i$. Thus, the first equality of (1.31) is proved. The inclusion $\mathrm{N}_{L/K}(1+\mathfrak{m}_L^{j+1}) \subset 1+\mathfrak{m}_K^{i+1}$ is already proved and the other inclusion follows from $\mathrm{N}_{L/K}(1+\mathfrak{m}_L^{j+e_{L/K}}) = 1+\mathfrak{m}_K^{i+1}$.

The second line is just for the record and follows from Lemma 1.7.3.1. The commutative diagram (1.32) follows from (1.34) and (1.30) with $\mathfrak{m}_K^i$ replaced by $\mathfrak{m}_K^{i+1}$ for $q = 2, \ldots, p-1$ in Lemma 1.8.4.2.

2. By $j \leqq m_{L/K}$, we have $d_{L/K} \geqq (p-1)j$ and $j - 1 \geqq e_{L/K}(f_{L/K} \cdot j - 1) - d_{L/K} = e_{L/K} \cdot (i-1) - d_{L/K}$. Since $f_{L/K} \cdot j = i$, similarly as in the proof of 1, we have $\mathrm{N}_{L/K}(1+\mathfrak{m}_L^j) \subset 1+\mathfrak{m}_K^i$ by Lemma 1.8.4.1. From this and 1, we have $\mathrm{N}_{L/K}(1+\mathfrak{m}_L^{j+1}) \subset 1+\mathfrak{m}_K^{i+1}$.

We have $2j - 1 \geqq j \geqq p \cdot j - d_{L/K} = e_{L/K} \cdot i - d_{L/K}$ for $j \leqq m_{L/K}$ and $j - 1 > e_{L/K} \cdot (i-1) - d_{L/K}$ for $j < m_{L/K}$. Hence the commutative diagram (1.33) follows from (1.30) with $\mathfrak{m}_K^i$ replaced by $\mathfrak{m}_K^{i+1}$ for $q = 2, \ldots, p-1$ in Lemma 1.8.4.2 similarly as in the proof of 1. □

Corollary 1.8.6. *Let K be a henselian discrete valuation field and let L be a wildly ramified cyclic extension of K of Galois group G. Let $d_{L/K}$, $e_{L/K}$ denote the valuation of the logarithmic different and the ramification index and let $m_{L/K} \geqq 1$ denote the largest integer such that $G_m \neq 1$. Then, for an integer $j > m_{L/K}$ such that $e_{L/K} \mid j + d_{L/K} = e_{L/K} \cdot i$, we have*

$$\begin{aligned} \mathrm{N}_{L/K}(1+\mathfrak{m}_L^j) &= 1+\mathfrak{m}_K^i, \qquad \mathrm{N}_{L/K}(1+\mathfrak{m}_L^{j+1}) = 1+\mathfrak{m}_K^{i+1}, \\ \mathrm{Tr}_{L/K}(1+\mathfrak{m}_L^j) &= 1+\mathfrak{m}_K^i, \qquad \mathrm{Tr}_{L/K}(1+\mathfrak{m}_L^{j+1}) = 1+\mathfrak{m}_K^{i+1} \end{aligned} \tag{1.35}$$

and the diagram

$$\begin{array}{ccc} \mathfrak{m}_L^j/\mathfrak{m}_L^{j+1} & \longrightarrow & 1+\mathfrak{m}_L^j/1+\mathfrak{m}_L^{j+1} \\ {\scriptstyle \mathrm{Tr}_{L/K}}\downarrow & & \downarrow{\scriptstyle \mathrm{N}_{L/K}} \\ \mathfrak{m}_K^i/\mathfrak{m}_K^{i+1} & \longrightarrow & 1+\mathfrak{m}_K^i/1+\mathfrak{m}_K^{i+1} \end{array} \tag{1.36}$$

is commutative.

Proof. By Proposition 1.8.3.2, we may replace K by the maximum tamely ramified extension K' in L, we may assume that L is purely wildly ramified and $[L:K]$ is a power of p. The case $[L:K] = p$ is Proposition 1.8.5.1. We show the case $[L:K] = p^e$ by induction on e. Assume $e \geqq 2$ and let M be the subextension such that $[L:M] = p$. Since $d_{L/K} = d_{L/M} + e_{L/M} \cdot d_{M/K}$, the assumption $e_{L/K} \mid j + d_{L/K} = j + d_{L/M} + e_{L/M} \cdot d_{M/K}$ implies that $e_{L/M} \mid j + d_{L/M} = e_{L/M} \cdot j'$. Hence by Proposition 1.8.5.1, we have

$$\mathrm{N}_{L/M}(1+\mathfrak{m}_L^j) = 1+\mathfrak{m}_M^{j'}, \qquad \mathrm{N}_{L/M}(1+\mathfrak{m}_L^{j+1}) = 1+\mathfrak{m}_M^{j'+1}$$

and the corresponding diagram (1.36) is commutative.

Since $j > m_{L/M}$ and $d_{L/M} + m_{L/K} = p \cdot m_{L/K}$ by (1.24), the inequalty $f_{L/M} \cdot m_{L/K} > m_{M/K}$ (1.20) implies $e_{L/M} \cdot j' = j + d_{L/M} > m_{L/K} + d_{L/M} = p \cdot m_{L/K} = e_{L/M} f_{L/M} \cdot m_{L/K} > e_{L/M} \cdot m_{M/K}$. Hence by the induction hypothesis, we have

$$\mathrm{N}_{M/K}(1+\mathfrak{m}_M^{j'}) = 1+\mathfrak{m}_K^i, \qquad \mathrm{N}_{M/K}(1+\mathfrak{m}_M^{j'+1}) = 1+\mathfrak{m}_K^{i+1}$$

and the corresponding diagram (1.36) is commutative.

□

Corollary 1.8.7. *Let K be a henselian discrete valuation field and assume that the residue field F is algebraically closed. Let L be a finite separable extension of K. Then, the norm mapping $\mathrm{N}_{L/K}\colon L^\times \to K^\times$ is a surjection.*

Proof. By replacing L by its Galois closure over K, we may assume that L is a Galois extension. Set $n = [L : K] = e_{L/K}$. Since the norm mapping induces the identity on $\mathbf{Z} = L^\times/\mathcal{O}_L^\times \to \mathbf{Z} = K^\times/\mathcal{O}_K^\times$ and the n-th power mapping on $E^\times \to F^\times$, it suffices to show that $1 + \mathfrak{m}_L \to 1 + \mathfrak{m}_K$ is a surjection. If L is tamely ramified, the assertion follows from Proposition 1.8.3.2 (1)⇒(3). Hence, by replacing K by the maximum tamely ramified extension in L, we may assume that the Galois group $G = \mathrm{Gal}(L/K)$ is a p-group. Since a p-group G is nilpotent, by induction on the order $\#G$, we may assume that L is a totally ramified cyclic extension of degree $p = \mathrm{char}\, F > 0$.

Let $m_{L/K}$ be the largest integer i such that $G_i = G$ as in Proposition 1.8.5. Then, by Proposition 1.8.5.2, we have $\mathrm{N}_{L/K}(1 + \mathfrak{m}_L^{m_{L/K}+1}) = 1 + \mathfrak{m}_K^{m_{L/K}+1}$. For $i = j = m_{L/K}$, the diagram

$$\begin{array}{ccc} \mathfrak{m}_L^i/\mathfrak{m}_L^{i+1} & \longrightarrow & (1+\mathfrak{m}_L^i)/(1+\mathfrak{m}_L^{i+1}) \\ \big\downarrow & & \big\downarrow{\scriptstyle \mathrm{N}_{L/K}} \\ \mathfrak{m}_K^j/\mathfrak{m}_K^{j+1} & \longrightarrow & (1+\mathfrak{m}_K^j)/(1+\mathfrak{m}_K^{j+1}) \end{array} \tag{1.37}$$

is commutative if we define the left vertical arrow by $\mathrm{Tr}_{L/K} + \mathrm{N}_{L/K}$. For $1 \leqq i = j < m_{L/K}$, the diagram (1.37) is commutative if we define the left vertical arrow by $\mathrm{N}_{L/K}$. Since $\mathrm{Tr}_{L/K}$ is an isomorphism and $\mathrm{N}_{L/K}$ is the p-th power mapping, the left vertical arrows are surjections by the assumption that F is algebraically closed. Hence we have $\mathrm{N}_{L/K}(1 + \mathfrak{m}_L) = 1 + \mathfrak{m}_K$ as required. □

Exercise 1.8. Let p be a prime number and $n \geqq 1$ be an integer. Show the inclusion $\mathrm{N}_{\mathbf{Q}_p(\zeta_{p^n})/\mathbf{Q}_p}\mathbf{Q}_p(\zeta_{p^n}^\times) \supset \langle p\rangle \cdot (1 + p^n\mathbf{Z}_p)$.

(We will see in Exercise 2.2 that the inclusion is in fact an equality.)

Solution. We have $[\mathbf{Q}_p(\zeta_{p^n}^\times) : \mathbf{Q}_p] = \#(\mathbf{Z}_p/p^n\mathbf{Z}_p)^\times = (p-1)p^{n-1}$. If $p \neq 2$, we have $1 + p^n\mathbf{Z}_p = \mathrm{Ker}(\mathbf{Z}_p^\times \to (\mathbf{Z}_p/p^n\mathbf{Z}_p)^\times) \subset \mathbf{Q}_p^{\times(p-1)p^{n-1}} \subset \mathrm{N}_{\mathbf{Q}_p(\zeta_{p^n})/\mathbf{Q}_p}\mathbf{Q}_p(\zeta_{p^n})^\times$. If $p = 2$, since $\mathrm{N}_{\mathbf{Q}_2(\zeta_4)/\mathbf{Q}_2}(1+2\zeta_4) = 5$, we have $1+2^n\mathbf{Z}_2 = \overline{\langle(1+5)^{2^{n-2}}\rangle} \subset \mathrm{N}_{\mathbf{Q}_2(\zeta_4)/\mathbf{Q}_2}\mathbf{Q}_2(\zeta_4)^{\times[\mathbf{Q}_2(\zeta_{2^n}):\mathbf{Q}_2(\zeta_4)]} \subset \mathrm{N}_{\mathbf{Q}_2(\zeta_{2^n})/\mathbf{Q}_2}\mathbf{Q}_2(\zeta_{2^n})^\times$. Since $\mathrm{N}_{\mathbf{Q}_p(\zeta_{p^n})/\mathbf{Q}_p}(\zeta_p - 1) = p$, we have the inclusion.

Historical notes

The definition of the lower ramification subgroups is given in [65, Chapitre IV §1 Proposition 1]. The shift of numbering by 1 is explained by Proposition 1.6.5.2.

The characterization by the different of tamely ramified extensions given in Lemma 1.7.4.1 is proved in [65, Chapitre III §7 Proposition 13] under the assumption that $\mathcal{O}_L$ is generated by a single element. The proof of the general case given here is taken from [1, Proposition A.3]. The equality (1.4) is attributed to Euler in [65, Chapitre III §6 Lemme 2].